(19) Europäisches Patentamt
European Patent Office
Office européen des brevets

(11) EP 0 542 298 B1

(12) EUROPEAN PATENT SPECIFICATION

(45) Date of publication and mention of the grant of the patent:
22.04.1998 Bulletin 1998/17

(51) Int Cl.[6]: **G06F 17/60**, G07F 7/10

(21) Application number: **92119461.9**

(22) Date of filing: **13.11.1992**

(54) Electronic monetary system

Elektronisches Zahlungsverkehrsystem

Système fiduciaire électronique

(84) Designated Contracting States:
AT BE CH DE DK ES FR GB GR IE IT LI LU MC NL PT SE

(30) Priority: **15.11.1991 US 794112**

(43) Date of publication of application:
19.05.1993 Bulletin 1993/20

(60) Divisional application: **97105388.9 / 0 788 066**
97105385.5 / 0 785 515
97105386.3 / 0 785 516
97105387.1 / 0 785 517

(73) Proprietor: **CITIBANK, N.A.**
New York, New York 10043 (US)

(72) Inventor: **Rosen, Sholom S.**
NY-New York 10024 (US)

(74) Representative: **Molyneaux, Martyn William et al**
c/o Ladas & Parry,
52-54 High Holborn
London WC1V 6RR (GB)

(56) References cited:
EP-A- 0 172 670
EP-A- 0 421 808
WO-A-83/03018
WO-A-91/16691
US-A- 4 320 387
US-A- 4 625 276

EP 0 542 298 B1

Printed by Jouve, 75001 PARIS (FR)

embodied as a national or international consumer banking system. The reference does not disclose any means for backing the electronic representations of economic value with equal valued liabilities as the counterpart to their assets.

European Patent Publication 421,808 discloses a system for transferring funds. The system uses a terminal under program control to move electronic representations of funds between portable data storage devices. The storage devices are embodied as "smart cards". The system allows the transfer of funds from a financial institution to a cardholder, from the cardholder to a retailer, and from the retailer to a second financial institution.

None of paperless payment systems that have been proposed so far are comprehensive enough so as to implement a multipurpose electronic monetary system that includes not only the automated devices that allow subscribers to transfer electronic funds or money between them without any intermediating system, but that also encompasses and includes an entire banking system for generating the value represented by the electronic money and for clearing and settling the electronic money accounts of the banks and financial institutions involved to maintain a monetary balance within the system.

Thus specifically, there is a need for a system that allows common payor to payee transactions without the intermediation of the banking system, and that gives control of the payment process to the individual. Furthermore, a need exists for providing a system of economic exchange that can be used by large organizations for commercial payments of any size, that does not have the limitations of the current EFT systems.

Accordingly, it is an object of the present invention to overcome the aforesaid shortfalls by providing a complete electronic monetary system which utilizes electronic money that is interchangeable with traditional cash and is universally accepted.

The electronic monetary systems according to the present invention are defined by the appended independent claims.

The present invention provides for securely transferring economic value including currency and credit among subscribers, among financial institutions, and between subscribers and financial institutions. The system provided is a paperless system whereby transactions can be carried out in both an on-line and an off-line mode between subscribers. The system reduces the cost of central electronic funds transfer systems by off loading much of the payments to off-line devices. The system provides for inexpensive electronic transfers to reduce an institution's cost of managing paper cash, checks and coins. Further, the invention provides a user friendly electronic payment system that may be used reliably and securely for real time transfers of money between members of the general public, between members of the general public and commercial organizations, and between commercial organizations. The system may be integrated with a wide variety of data processing and data communication systems including currently available home banking services. Further, the system can be utilized with electronic money in the form of multiple currencies and in transactions of virtually-any size denomination. Further the medium of economic exchange provided is fungible, easily transferable, undeniably redeemable, and secure from reuse, duplication, and counterfeiting.

The foregoing features and advantages of the invention are illustrative of those which can be achieved by the present invention and are not intended to be exhaustive or limiting of the possible advantages which can be realized. Thus, these and other features and advantages of the invention will be apparent from the description herein or can be learned from practicing the invention, both as embodied herein or as modified in view of any variations which may be apparent to those skilled in the art.

Summary of Exemplary Embodiment

To achieve the foregoing, and other objects, the apparatuses of the present invention employ a preferred embodiment in the form of an electronic-monetary system having (1) banks or financial institutions that are coupled to a money generator device for generating and issuing to subscribing customers electronic money including electronic currency backed by demand deposits and electronic credit authorizations; (2) correspondent banks that accept and distribute the electronic money; (3) a plurality of transaction devices that are used by subscribers for storing electronic money, for performing money transactions with the on-line systems of the participating banks or for exchanging electronic money with other like transaction devices in off-line transactions; (4) teller devices, associated with the issuing and correspondent banks, for process handling and interfacing the transaction devices to the issuing and correspondent banks, and for interfacing between the issuing and correspondent banks themselves; (5) a clearing bank for balancing the electronic money accounts of the different issuing banks; (6) a data communications network for providing communications services to all components of the system; and (7) a security arrangement for maintaining the integrity of the system, and for detecting counterfeiting and tampering within the system.

In the preferred embodiment the functions of the money generating devices, the transaction devices, and the teller devices will be performed by a combination of tamper-proof computer hardware and application software modules that may be networked together. Information is transmitted in an encrypted form to provide security from unauthorized inspection. The electronic money is transmitted with digital signatures to provide authentication, and security from modification or counterfeiting.

Figure 8 is a block diagram of a Network Server, according to the invention.
Figure 9 is a flow diagram of the security server, according to the invention.
Figure 10 is a block form diagram of the security server, according to the invention.
Figure 11-24 are flow diagrams of accounting examples, according to the invention.
Figure 25 a flow diagram of the Transaction Reconciliation System, according to the invention.
Figure 26 is a flow diagram of the Clearing System, according to the invention.
Figure 27 is a flow diagram of the Money Issued Reconciliation System, according to the invention.
Figure 28-50A are flow charts of transaction examples, according to the invention.

Disclosure of the Preferred Embodiment the Invention

The present invention contemplates an improved monetary system using electronic media to securely and reliably exchange economic value. The system can be implemented by integrating novel data processing systems with other procedures which can be implemented with the current worldwide banking systems.

Throughout this description, "electronic money" may also be referred to by the abbreviation "E-M." Additionally, the term "bank" is used hereinafter to indicate any banking, financial institution or the like which is a participant of the present invention.

Referring now to the drawings, wherein like numerals refer to like components, there is disclosed in Figure 1, in block form, broad aspects of the preferred embodiment. In Fig. 1, the general relationship among the features of the system is shown. The system includes Issuing Banks **1** each having a Teller money module **5** and a Money Generator module **6**; Correspondent Banks **2** each having a Teller money module **5**; an electronic money Clearing Bank **3**; a Certification Agency **28** and a plurality of Transaction money modules **4** owned by subscribers of the system. Though money generator module **6** and teller module **5** are preferably embodied separately, the functions of these modules may be embodied in a unitary device processor control.

Electronic notes **11**, the media for transferring electronic money, are generated by the Money Generator module **6** for an Issuing Bank **1**. Theses notes **11** are then transferred by a Teller money module **5** to a subscriber utilizing a Transaction money module **4**. Electronic notes may be representations of currency or credit authorizations For security reasons, all electronic notes **11** will expire after a preset time period. Once expired, the notes **11** must be redeemed at a participating bank for updated ones before they can be transferred.

An Issuing Bank **1** generates and distributes the electronic notes **11**, and is liable for their redemption. An Issuing Bank **1** performs deposits, withdrawals, payments to loans and inquiries for other money modules.

A Correspondent Bank **2** is a participating bank which distributes electronic money through accounts it maintains at Issuing Banks **1**, but does not generate any electronic money, and is not liable for its redemption. Because it cannot generate any electronic money, the Correspondent Bank **2** in the preferred embodiment must make real-time requests of electronic money from an account it maintains at an Issuing Bank **1** whenever a subscriber wishes to withdraw electronic money at a Correspondent Bank **2**.

Conversely, a Correspondent Bank **2** deposits all electronic money deposited by subscribers, to the accounts the Correspondent Bank **2** holds at Issuing Banks **1**. These accounts will be described hereinafter. A Correspondent Bank **2**, like an Issuing Bank **1**, will perform deposits withdrawals, payments to loans and bank inquiries.

Notably, an Issuing Bank **1** may also be a Correspondent Bank **2** for the monetary units that it does not generate. For example, an Issuing Bank **1** for electronic dollar notes **11** may be a Correspondent Bank **2** for electronic notes **11** of yen, marks, issued by other banks etc.

It is also important to note that the system of the invention can function without correspondent Banks **2**. For example, a subscriber can eliminate the use of a Correspondent Bank **2** by communicating directly with his/her Issuing Bank **1** when making a deposit, withdrawal, etc. Correspondent Banks **2** are included in the preferred embodiment for the practical purpose of expanding distribution of the system while reducing the risks that are inherent in any banking system, such as the risks caused by the collapse of a bank issuing money.

The Clearing Bank **3** is utilized when more than one bank is issuing electronic money. According to the invention, it is anticipated that more than one bank will be issuing electronic money. Thus, the Clearing Bank **3** is provided to clear the electronic money deposited and to balance accounts it maintains for the Issuing Banks **1**. The Clearing Bank **3** maintains demand accounts for each Issuing Bank **1** in the system.

The Certification Agency **28**, is the centerpiece of the system security. It provides a process that "certifies" the validity of a money module for a certain period of time by issuing a certificate to each money module. A money module must have a valid certificate in order to be able to transact with other money modules **4**, **5**, **6**.

Before the certificate expires, it must be updated so that a subscriber can continue to use his/her transaction money module **4**. This process makes users of the system establish periodic contact with the Certification Agency **28**.

Periodic contact allows for faster response when tampering with the money modules of the system is detected. To this end, the Certification Agency **28** also provides a list of offending or compromised money modules to other money

Transaction Reconciliation System 22 and an Issuing Bank's 1 Money Issued Reconciliation System 23 for maintaining statistical and housekeeping functions. Records of the electronic notes 11 cleared and settled at the Clearing Bank 3 are also provided to the Money Issued Reconciliation System 23 . From these compilations, a financial position of the system can be produced by the Money Position System 24.

Discrepancies and malfunctions are reported to the Security System 21 which downloads the lists of problem money modules to all money modules in the system when they are connected to the Network 25. By carrying this list, a Transaction money module 4 will be inhibited from transacting with other suspect Transaction money modules 4.

Having thus provided an overview of the preferred embodiment, there will now follow a more detailed description of the individual elements and the transactions between them.

Money modules

Figure 3 provides several embodiments of external systems or devices for housing money modules.

In the preferred embodiment, the external system or device will typically contain data display means, data input means, data processing means, memory storage means, direct connection or contactless bidirectional communications means, and the money module packaged in a tamper - proof housing, all interfaced by suitable means for information transfer, such as are well known in the art.

As will be understood, a money module may be embodied as a modular component of any larger processing environment while still performing the same functions. For example, Transaction money modules 4 may work as co-processors embedded in personal portable computer devices like the Hewlett-Packard 95LX, or as coprocessors in mainframe computers, workstations, point-of-sale terminals or telephone devices (fixed or portable) connected to a network.

A Teller money module 5 may be embodied as a co-processor in the bank's financial computer systems. The Money Generator module 6 could be a separate processing unit networked to the bank, a co- processor in a general unit networked to the bank, a co-processor in a general purpose computer, or it may be combined with an Issuing Bank's 1 Teller money module 5 in a larger processor as illustrated by the unitary device 1001 of Figure 1--.

Because it is anticipated that a money module will be implemented in a separate processing device, it is assumed that corresponding interface circuitry would be provided in the host processing device to provide communication between the processing device and the money module.

Notably, all classes of money modules contemplated by the invention may be implemented programmatically or by direct electrical connection through customized integrated circuits, or a combination of both, using any of the methods known in the industry for providing the functions described below without departing from the teachings of the invention. Those skilled in the art will appreciate that from the disclosure of the invention provided herein, commercial semiconductor integrated circuit technology would suggest numerous alternatives for actual implementation of the inventive functions of the money module that would still be within the scope of the invention.

Transaction Money Module

In one embodiment, the Transaction money module 4 may be imbedded in any computer of any size or use, like those serving as general purpose computers or work-stations, to provide functions not limited to E-M transaction use. This latter application will allow for such uses as real-time, off-line payments between personal computing devices, or on-line payments for network services such as information retrieval, telephone calls, or for purchasing airline tickets, theater tickets, etc.

In another embodiment, the Transaction money module 4 may be imbedded in an individual hand-held integrated circuit unit, such as a personalized hand-held computer that may be readily carried by an individual as though it were a wallet. As an illustration, the device of the preferred embodiment may include a keyboard, a pen or stylus, a touch screen or voice recognition circuitry as a data input means, an alphanumeric LCD dot matrix display as a display means, an infrared optical transceiver as a contactless bidirectional communications means, and an RJ-11 telephone jack coupled to modem circuitry as a telephonic communications means. Additionally, the device may also include various electronic processing and storage means for providing calculator capabilities, for storage and processing data of the owner, etc.

It is important to note that the particular design of the external device is not critical to the invention, and other technologies suitable for accomplishing the foregoing functions may also be used. For example, an LED instead of an LCD display panel may be used; radio, infrared, inductive or capacitive communications methods may be used instead of direct connection, optical communications methods may be used; etc.

In general, it is anticipated that any Transaction money module 4 owned by a subscriber will be embodied in a self-contained, tamper-resistant unit that contains components which are difficult to access, and thus prevent any person from improperly examining, counterfeiting or modifying any of its contents or arrangements. For example, in-

In the preferred embodiment, every money module will have an identifier. A money module identifier may be thought of as the "serial number" of the money module and is never changed.

It is anticipated that a subscriber may have access to several of the fields of data stored in the Tran Log application, such as histories of the amount, date, and type of transfer. Information as to the expiration date of a certificate may also be accessed by the subscriber so that he/she will be informed as to the need to update or revalidate the money module's certificate.

The Maintain Security application **37** manages a list of money module identifiers that are known to have been generally compromised. In particular, this is a list that is distributed to each money module when it communicates with the Network **25**, and is a list of money modules that have passed an invalid or counterfeit electronic note **11** or have performed acts deemed detrimental to the system.

When establishing a session between money modules, each money module checks its list of bad money modules to see if the other is an offending money module. If the other money module's identifier appears on the list, the communication is broken off.

This application also provides the process for obtaining the certificate unique to the money module, for synchronizing the internal clock, and for managing the creation of new cryptography keys.

The Note Directory **39** application performs the function of keeping track of the location, identification and value of each of the electronic notes **11** stored within the money module. A note **11**, whether it is an electronic currency note or an electronic credit note, is the basic unit of electronic money. It is the electronic object representing the economic value, the electronic bits that contain the amount, expiration date, note identifier etc. (described in detail below) that gets digitally signed (described below) and encrypted when being transferred. Both electronic currency notes **11** and electronic credit notes **11** may be located by the Note Directory **39**.

The Note Directory application **39** updates the current amounts of electronic notes **11** (both currency and credit), after every transfer. A date-of-expiration, a note identification number and an Issuing Bank identifier is also recorded with the location of each note **11**.

In summary, the Note Directory **39** keeps track of the note identification number, the Issuing Bank **1** identifier, the date-of-expiration of the note **11**, the location of the note **11** as stored in the Transaction money module **4**, and the current amounts of the value of each of the notes **11** stored. These records are maintained for both electronic currency and electronic credit. For a credit note **11**, the account number of the credit line is also maintained.

The Notes application **40** manages the storage of the representations of the electronic notes **11** themselves, both currency and credit notes **11**. This application also generates the transfers when notes **11** are to be conveyed.

The Packet Manager application **41** manages the construction and formatting of a packet of electronic notes **11** that are to be transferred to another money module. For example, the Packet Manager **41** will utilize an algorithm so that the least number of electronic notes **11** are used to fulfill the requested amount of transfer, with the earliest dated electronic notes **11** being used first. Alternatively, when a packet of notes **11** is transferred to the receiving money module, the Packet Manager **41** application "disassembles" the packet, verifying the date and separating the data fields that represent the different electronic notes **11**.

The formatted packet gets several data fields appended to it when electronic notes **11** are "assembled." An identifier data field provides the indicia that identifies it as a packet. Additionally, data fields for the total value of the notes **11**, the number of notes **11**, and the individual locations of the notes **11** are provided.

The Verifier application **42** verifies that a received packet contains valid electronic notes **11** before a receiving money module accepts them. The Verifier **42** also checks that the total amount received is equal to the sum of the electronic notes **11** that are to be transferred. If the total amount and the individual electronic notes **11** are valid, an acknowledgment is returned to allow for completion of the transfer. Otherwise, an "invalid" message is sent, and the transfer may be aborted.

Services applications that are provided fall under two categories: Clock/Timer **43** and Cryptography. The Clock/Timer **43** provides output pulses for controlling a transaction timeout, such as the time between the sending of a message and the return of a corresponding message.

As will be appreciated, when two money modules are communicating, they may be monitoring a time-out protocol. For example, after a first money module has sent a message to a second money module, the Session Manager **31** of the first money module ("A") may set a timer for a reply if the Transactor **32** indicates that a reply is required. The Session Manager **31** may also number the message sent. This number would appear in the reply message from the Session Manager **31** of the second money module ("B").

If the timer expires before the message has been received, then Session Manager A **31** will query Session Manager B **31** to determine if the transaction is still running in B. If B does not reply then Session Manager A **31** will abort the transaction. If a reply is received that the transaction is proceeding, then the timer will be reset to a new time. If A queries B a predetermined number of times without receiving a reply to the original message, then A may abort the transaction.

Separately, this application also maintains the current date and time, both for user display and for verifying that

security involved.

The Teller money module **5** contains an External Interface **30**, a Session Manager **31**, a Transactor **32** and a Money Holder **38** that perform similar functions to the corresponding components in the Transaction money module **4** described above.

Briefly, the External Interface **30** interfaces the Teller money module **5** to other processing and communications means within the Teller money module **5** host processor; the Session Manager **31** acts to control and commit (i.e., finalize) or abort a transaction session between the Teller money module **5** and another money module; the Money Holder **38** manages the storing and retrieval of electronic money; and the Transactor **32** manages the application functions of a To Teller **34**, the Tran Log Mgr. **36**, the Maintain Security **37**, the To Bank **47**, a To Money Generator **48**, and the To Transaction **49**. .

The following list describes in brief, the applications contained in the Teller money module **5** that are functionally identical to the applications found in the Transaction money module **4**:

- To Teller **34**: Interfaces deposit and withdrawal functions to another Teller money module **5**.
- Tran Log Mgr. **36**: Transaction log manager for recording transaction details.
- Maintain Security **37**: Manages the list of compromised money modules, applies for certificates, synchronizes the clocks, and manages the creation of new digital keys.
- Note Directory **39**: Keeps track of the location, value and identification of notes **11** by monetary unit. Summary totals are also maintained.
- Notes **40**: Manages storage for the electronic notes **11** of exchange, and creates the transfers for the notes **11**.
- Packet Manager **41**: Manages the assembly and dissembly of a packet to be transferred to a different money module.
- Verifier **42**: Verifies that a received packet contains valid electronic notes **11**.
- Clock/Timer **43**: Controls transaction timeout, expiration of the validity of the electronic notes **11**, expiration of the certificate, and general clock functions.
- Cryptography

  (i) Public key **44**: used for signatures to sign and validate notes **11** and to set up a secure transaction session.
  (ii) Symmetric key **45**: Controls the security of a transaction session.
  (iii) Random number generator **46**: Generates random like numbers for new cryptographic keys.

Some of the distinguishing applications are the To Bank **47** and To Transaction **49** applications. The To Bank application **47** provides the interfacing means whereby the Teller money module **5** can perform exchanges of data for inquiries and account postings with the on-line systems of a bank. This application is also utilized for crosschecking the customer's account number with the accounts and type of transaction being requested.

The To Transaction application **49** performs deposits, withdrawals and payments to loans. This application operates whenever a Teller money module **5** is transacting with a subscriber's Transaction money module **4**.

As mentioned above, a Teller money module **5** may be associated with an Issuing Bank **1** or a Correspondent Bank **2**. When Teller money module **5** is associated with a Correspondent Bank **2**, it is utilized for intermediating deposits, withdrawals, and payments to loan accounts between a Transaction money module **4**, the Correspondent Bank's **2** on-line systems, and an Teller money module **5** at an Issuing Bank **1**.

When operating in an Issuing Bank **1** mode, the Teller money module **5** is used for intermediating deposits, withdrawals, and payments to loan accounts between other money modules and the Issuing Bank's **1** on-line systems. Additionally, when the Teller money module **5** is performing in an Issuing Bank **1** mode, a To Money Generator application **48** may be employed when requesting new notes **11**.

Basically, the To Money Generator application **48** performs banking functions dealing with requests for electronic notes **11**. It interfaces an Issuing Bank's **1** Teller money module **5** to a Money Generator Module **6**.

All of the other elements performed in an Issuing Bank's **1** Teller money module **5** are essentially identical to the similarly named components and application functions described above.

Money Generator Module

Figure 6 is a block diagram illustrating the application functions of a Money Generator module **6**. Money Generator modules **6** provide the mechanism that Issuing Banks **1** utilize to issue electronic money. A Money Generator module **6** is also encased in a tamper-resistant package for the same security reasons stated above for other money modules.

A Money Generator module **6** generates the electronic money (in the form of electronic notes **11**, to be described in further detail below), and distributes them to other money modules through the Teller money module **5** of an Issuing Bank **1**. The Money Generator module **6** includes a unique application not present in other money modules for re-

(3) Manage Network Sign-on **58** - controls the money module Network sign-on process;
(4) Synchronized Time/Date **59** - keeps money module Clock/Timer **43** services synchronized to a system time;
(5) Route Message **60** - directory services for routing messages, controlling message routing during sign-on and during a money module session; and
(6) Direct to Bank Services **61** - provides information on services provided by participating banks.

As will be appreciated by one skilled in the art, switching and processing centers that are known in the industry may be used to enable the networking cooperation between a financial institution and any other that is coupled to the same centers.

Electronic notes

We turn now to a further description of the elements of the electronic notes **11** themselves.

An electronic currency note **11** representing value is essentially an electronic object created from a transaction request (deposit or withdrawal) which is backed by demand deposits at an Issuing Bank **1**. At various times and in various points of the system, the notes may appear in electrical or magnetic forms or as electromagnetic radiation. These notes **11** may be transferred over several transactions just like paper money, with the additional property of fungibility that allows the electronic notes **11** to be commuted and transferred in amounts less than or equal to the value of the note **11**.

Notes **11** may be split by appending a transfer record to the note **11** and signing the note **11** using the private cryptographic key of the money module transferring the note **11**. Electronic credit notes **11**, however, can only be transferred once in the preferred embodiment, because it is anticipated that its receiver must deposit the credit note **11** so that the loan may be realized.

Credit notes **11**, unlike currency notes **11** are drawn on a subscriber's loan account. Each credit note **11** carries the account number it is drawn on. The account may be a revolving credit or credit line on which the note **11** is drawn, operating much in the same way that a check or a credit card account works in today's banking industry. Credit notes **11** can represent a part of or all of the credit line of the account.

In the preferred embodiment, the credit notes **11** can only be transferred to another Transaction money module **4** by the owner of the account, and the receiver of a credit note **11** can only deposit it into his or her account as currency. From there, the credit note **11** is cleared with the currency at the Clearing Bank **3**. The subscriber's bank recognizes the loan upon receipt of the cleared credit note **11**.

When credit notes **11** are withdrawn, they do not trigger any accounting transactions in the preferred embodiment. Current credit line processing may need to be modified to keep track of the amount of the credit line in the subscriber's Transaction money module **4**. Whenever the subscriber communicates with the Issuing Bank **1** maintaining the credit line, the amount of the credit line in the Transaction money module **4** is removed and replaced based on any adjustments to the credit line in the banking system **20**. Total credit notes **11** plus outstanding loans must be less than or equal to the total amount of the credit line.

Electronic notes **11** are comprised of three collections of data fields, namely a Body group, a Transfer group, and a Signatures and Certificate group. The Body group of data fields includes the following information:

(1) the type of electronic note **11**, i.e., whether it is a currency note **11** or a credit note **11**;
(2) the Issuing Bank's **1** identifier;
(3) the monetary unit identifier;
(4) a Note identifier;
(5) its date-of-issue;.
(6) its date-of-expiration;
(7) the subscriber's account number (used only for credit notes **11**);
(8) the amount or value of the note **11**; and
(9) the Money Generator module **6** identifier.

The Transfer group of data fields includes:

(1) a total of the number of times that the electronic note **11** was transferred; (provided for currency notes **11** only)
(2) a list of transfer records that indicate the date-of-transfer, the amount transferred and the identification number of the receiver.

The Signature and Certificates group of data fields includes:

modules **4** access the Certification Agency **28** on a periodic basis to obtain the latest list. Placing a time limit on the Transaction money module's **4** ability to transact (in addition to the time limit placed on electronic notes **11**) will force subscribers to access the Certification Agency **28** through the Network **25** on a periodic basis to receive the latest bad money module list along with a new certificate. Advantageously, the period of the certificate validity can be closely monitored and adjusted according to security needs.

The Certification Agency **28** distributes its updated certificatory key and money module certificates on-line through the Security Server **27** (see Figure 9). An important component of the system's security is provided by Security Servers **27** at the participating banks and Security Servers **27** at the Certification Agency **28**.

Referring now to Figure 10, a block diagram of a preferred embodiment of the Security Server **27** is shown. It is contemplated that the Security Server **27** at the Certification Agency **28** or on a bank's local network **18** will contain the following application functions:

(1) External Interface **54** - a communications layer for connecting to a bank's local network **18** or the Certification Agency's local network **17**;
(2) Session Manager **55** - controls the security aspects of a transaction session;
(3) Create Certificate **50** - certifies a certificate for any of the money modules;
(4) Create Account Profile **51** - certifies and signs a bank account profile (described in detail hereinafter) that allows a Transaction money module **4** to access the subscriber's different bank accounts;
(5) Distribute Certification Keys **52** -distributes the Certification Agency's **28** list of valid public keys to the money modules;
(6) Bad Money Module Control **53** - controls and distributes the list of bad money modules; and
(7) Services - identical to the cryptographic functions **44, 45, 46** in the money modules described above

Since certificates will expire over time, money modules will be required to apply for new certificates periodically. In order to receive a new certificate, the money module creates a new public key and private key. The new public key, the money module identifier and the old certificate are presented to the Certification Agency **28** after being digitally signed using the old private key.

The Certification Agency **28** checks the signature and if it is valid, signs the new public key and identifier and sends the certificate to the money module with a future expiration date. The Certification Agency's **28** Security Server **27** also distributes a list of bad money modules via the Network **25**. Initially, each participating bank's Security Server **27** reports the identifiers of money modules which hold notes **11** invalidly or that are counterfeit. Those identifiers are passed through the Security Servers **27** and are compiled by the Certification Agency **28**.

All such identifiers are distributed to the Teller and Money Generator modules **5, 6** respectively. A money module will not transact with another money module found on the list of bad money modules. Optionally, only those money modules which have demonstrated a flagrant breach of security will be distributed to Transaction money modules **4**.

If a Transaction money module **4** is lost or stolen, the subscriber would report it to his/her bank or to the Certification Agency **28** so that the money module identifier may be placed on the bad money module list to inhibit any further transactions.

While the security of the system is provided by being able to block a money module from transacting, system security is also maintained by providing the expiration date on the electronic notes **11** in addition to the money module certificates.

As mentioned previously, a note **11** will be valid only for a limited time period after it is generated. Its date-of-expiration is a security parameter which may also be monitored and varied as needed. The period of validity of a note **11** can be varied by the value of the note **11**. Preferably, a large note **11** will expire in a shorter time period than a smaller one. For example, a $1,000,000 note may be set to expire five days after the date of its creation since it would provide a significant incentive to counterfeit, while a $50 note **11** may be set to expire after a month from the date of its creation.

A Transaction money module **4** will not accept expired notes **11**, but can deposit or exchange the notes **11** it may contain for new notes **11**. The expiration dates are checked by the Verifier **42** and Clock/Timer **43** applications in a money module before any electronic note **11** is transferred. Separately, it is also anticipated that if the money module loses power then it will not be able to pay or exchange notes **11** after power has been regained until it has communicated again with the Network **25** and had its security parameters updated.

As stated above, a subscriber will typically obtain a Transaction money module **4** already loaded with a certificate. Securing the Transaction money module **4** itself to a subscriber may be accomplished by assigning it a unique PIN, biometrics or other personal secret characteristics.

Before any personalization of the money module **4** may proceed, the Transaction money module **4** checks if there is a bank account already stored in the To Teller **34** application or if the Notes **40** application contains any electronic notes **11**. In either of these cases, the Transaction money module **4** will inhibit the subscriber from securing the module

at a branch, or over the telephone utilizing a special dialogue. For example, the subscriber may identify himself by his PAN and PIN. He may then enter each account number he wishes to access from his Transaction money module **4**. The account numbers may be verified in the bank's account reference files. A cross-reference of accounts to Transaction money modules **4** may be maintained by each bank if they so choose.

The composition of an exemplary account profile may be:

(1) Bank Identifier -- one for each bank;
(2) Account Numbers;
(3) Account Types -- e.g., checking, savings, credit; and
(4) Security Server's **27** signature on the list of accounts.

It will be understood that the list of account numbers will be digitally signed by the bank Security Server **27**. As a further security measure the account profile may be re-signed with an updated public key on a periodic basis. The fundamental access security is provided by the digital signature of the bank's Security Server **27**.

Banking System (Accounting Architecture)

It is a notable feature of the preferred embodiment, that the method of the system can parallel the existing and varying types of accounting methods that exist today. The system of the preferred embodiment follows the various types of accounting methods practiced presently in various banks. However, it is important to note that unlike the present banking system, in the preferred embodiment of the invention, economic value is created on demand. Thus, there is no inventory of cash or checks involved; electronic currency from demand deposits and electronic credit are created on a real-time basis. This elimination of a paper inventory by using an electronic media of exchange requires certain supplements to the commonly practiced accounting techniques to provide the real-time accounting needed.

Accordingly, the embodiment of the present invention provides an accounting structure to supplement those used in the present banking systems **20**. The improved accounting arrangement may be utilized to monitor the electronic money and each bank's obligation when a financial transaction between a Transaction money module **4** and a Teller money module **5** occurs, or when a Clearing Bank **3** performs any clearing processes.

When electronic notes **11** are transferred to or from a Teller money module **5**, in most cases accounting transactions affecting the records of the banking system **20** are created. Conversely, transfers between Transaction money modules **4** do not involve any formal accounting procedures -- they involve only the transfer of electronic notes **11**.

In the system being described, it is anticipated that the following arrangements of accounts are to be utilized for each type of bank, categorized under each monetary unit:

At an Issuing Bank **1**-

(1) Money Issued Account: A liability account which reflects the money issued but not cleared.
(2) Money Due Account: An asset account reflecting the money deposited to the bank's accounts.
(3) Deposited at Clearing Bank Account: An asset account reflecting the balance of a clearing account at a Clearing Bank **3**.
(4) Correspondent Bank Money Account: A liability account owned by a Correspondent Bank **2** which is drawn upon by the Correspondent Bank **2** to dispense electronic money.
(5) Money In Transit Account: A zero-balance liability account owned by each bank, which is used to temporarily maintain electronic money during a financial transaction.
(6) Foreign Exchange Account: A zero-balance liability account owned by each bank, which is used to handle multiple currency exchanges.

At a Correspondent Bank **2** -

(1) Deposited at Issuing Bank Account: An asset account reflecting the balance of the Correspondent Bank **2** account at the Issuing Bank **1**.
(2) Money Due Account: An asset account reflecting the money deposited to the bank's accounts.
(3) Foreign Exchange Account: A zero-balance liability account owned by each bank, which is used to handle multiple currency exchanges.
(4) Money In Transit Account: A zero-balance liability account owned by each bank, which is used to temporarily maintain electronic money during a financial transaction.

At the Clearing Bank **3**:

Alternatively, if a subscriber begins with $50 in his/her Transaction money module 4 and deposits all of it, the customer account would be credited $50 and the Money Due account would be debited by $50 (Step 1 of Figure 11; parenthetical entries).

When there are only $50 of electronic notes 11 that are removed, the Correspondent Bank 2 credits the Money Due account $50 and the Deposited at Issuing Bank account is debited $50 (Step 2, parenthetical entries). This money is then deposited at the Issuing Bank 1 for later clearing, wherein the Correspondent Bank Money account is credited by $50 and the Money Due account is debited by $50. Because no updated electronic notes 11 need be returned in this situation, the deposit and its corresponding accounting is completed at Step 2.

The accounting processes of an electronic money deposit at an Issuing Bank 1 instead of a Correspondent Bank involve fewer operational steps, which are illustrated in Figure 12. Using the same dollar amounts as in the previous exemplary transaction, when $50 of $100 in electronic money stored in the Transaction money module 4 are deposited directly to an Issuing Teller money module (Step 1), $50 would be credited to the customers account (A). Fifty dollars would simultaneously be credited to the Money In Transit account, and $100 would be debited to the Money Due account at the Issuing Bank 1.

Since the entire $100 stored in the Transaction money module 4 is removed and transferred to the Issuing Bank's Teller money module 5, it is necessary to return $50 of updated notes to the Transaction money module 4. Accordingly, as shown in Step 2 the Teller money module 5 requests $50 from its Money Generator module 6, debiting its Money In Transit account by $50 and crediting its Money Issued account by $50.

In response, $50 is created by the Money Generator module 6 and transferred to the Teller money module 5, which in turn transfers this electronic money to the Transaction money module 4 (Step 3-4).

When only $50 is stored in the Transaction money module 4 and all of it is deposited, the customer's account (A) is credited $50, the Money Due account is credited $50, and that is the end of it. See parenthetical entries in Step 2 in Figure 12.

In the case of a withdrawal from a Correspondent Bank (see Figure 13), a withdrawal request of $100 by a subscriber using a Transaction money module 4 at a Correspondent Bank 2 will cause the subscriber's account (A) to be debited by $100 and the Correspondent Bank's 2 Money In Transit account to be credited by $100 (Step 1). The request for the $100 withdrawal is forwarded to the Issuing Bank 1 from the Correspondent Bank 2, and the Correspondent Bank's Deposited at Issuing Bank account is credited by $100 while its Money In Transit account is debited by $100 (Step 3).

Next, the request for $100 is forwarded by the Issuing Bank's 1 Teller money module 5 to the Money Generator module 6. Accordingly, the Correspondent Bank Money account gets a $100 debit while the Money Issued account gets a $100 credit (Step 4).

The Money Generator module 6 then creates the $100 of electronic notes 11, and transfers it to the Transaction money module 4 via the Issuing Bank's 1 Teller money module 5 and the Correspondent Bank's 2 Teller money module 5 (Steps 5-6).

When, e.g., the subscriber makes the $100 withdrawal request with a Transaction Money Module 4 that contains $50 of electronic notes 11, the notes 11 are removed and now the Money Due account is debited $50, the subscriber's account is still debited $100, and the Money In Transit account is credited $150 (parenthetical entries, Step 1).

The $50 is then deposited to an Issuing Bank 1, causing the Money Due account to be credited $50 and the Deposited at Issuing Bank account to be debited by $50. At the Issuing Bank 1, the Correspondent Bank Money account is credited $50 while the Money Due account is debited $50 (Step 2, parenthetical entries).

Because $50 of notes 11 have been removed, the withdrawal request in Step 3 must be for $150. This request causes the Deposited at Issuing Bank account to be credited by $150 and the Money In Transit account to be debited by $150 (Step 3 parenthetical entries).

At the Issuing Bank, $150 is requested from the Money Generator Module 6 and the Correspondent Bank Money account gets a $150 debit while the Money Issued account gets a $150 credit (Step 4 parenthetical entries). As above, the money generated by the Money Generator Module 6 ($150) gets conveyed to the Transaction money module 4 via the Issuing Bank 1 and Correspondent Bank 2 Teller money modules 5 (Steps 5-6, parenthetical entries).

A withdrawal from an Issuing Bank 1 involves fewer accounting procedures. Referring now to Figure 14, a withdrawal request by a Transaction money module 4 from an Issuing Bank 1, Step 1 will cause the Issuing Bank 1 Teller money module 5 to debit the subscriber's account (A) by $100 and credit its Money Issued account by $100 (Step 1-2).

A request for an updated $100 is then made by the Issuing Bank's 1 Teller money module 5 to the Money Generator module 6, which upon its creation will return $100 to the Issuing Bank's Teller money module 5 (Step 3). In completing the transaction, the Issuing Bank's 1 Teller money module 5 simply transfers this $100 containing the most recent certificate to the Transaction money module 4 (Step 4).

Alternatively, when the Transaction money module contains $50 at the time of the $100 withdrawal, (parenthetical entries) the $50 will be removed, the Issuing Bank's Money In Transit account will be credited $50 and the Money Due account will be debited $50 (Step 1).

by $50. Since no notes 11 are removed, no accounting is performed in Step 2.

In Step 3, only $50 is requested from the Money Generator module 6, and the Money In Transit account is debited by $50 while the Money Issued account is credited by $50. The same transfer between money modules occurs as in Steps 4-5 of Fig. 19 described above, using only the $50 that was requested. This would leave the subscriber with $50 of electronic notes 11 in lieu of his original $50 of paper money.

In Fig. 20, an exchange of cash for electronic notes 11 at a Correspondent Bank 2 is shown. This example uses the same parameters as in Figure 19, namely, the subscriber has $50 of cash and $100 of electronic notes 11 in his Transaction money module 4.

When the $50 in cash is deposited to the Correspondent Bank 2, its Money In Transit account is credited $50 while its Cash account is debited $50 (Step 1). The $100 of electronic notes 11 is then transferred from the Transaction money module 4 to the Correspondent Bank 2 which credits its Money In Transit account by $100 and debits its Money Due account by $100 (Step 2).

From there, the $100 of electronic notes 11 is deposited at the Issuing Bank 1, wherein its Money Due account is debited by $100 while its Correspondent Bank Money account is credited by $100 (Step 3). At the Correspondent Bank 2, the Deposited at Issuing Bank account is debited by $100 while the Money Due account is credited by $100.

A withdrawal request is then made by the Correspondent Bank 2 for $150 from the Issuing Bank 1 (Step 4). This request results in the Correspondent Bank 2 debiting its Money In Transit account by $150 and crediting its Deposited at Issuing Bank account by $150.

Correspondingly, the Issuing Bank 1 Teller money module 5 requests $150 of notes 11 from the Money Generator Module 6, debits its Correspondent Bank Money account by $150 and credits its Money Issued account by $150 (Step 5).

Finally, the $150 of electronic notes 11 is transferred from the Money Generator module 6 to the Issuing Bank's 1 Teller money module 5 which transfers it to the Transaction money module 4 after passing through the Correspondent Bank's 2 Teller money module 5 (Steps 6-8).

Alternatively, a subscriber having only $50 of cash and no notes 11 in his/her Transaction money module 4 is also shown in Fig. 20. As in the first case, the $50 in cash is deposited to the Correspondent Bank 2, its Money In Transit account is credited $50 while its Cash account is debited $50 (Step 1).

A $50 withdrawal request is then made to the Issuing Bank 1, and the Money In Transit account is debited by $50 while the Deposited at Issuing Bank account is credited $50 (Step 4, parenthetical entry). Thereafter, $50 is requested from the Money Generator Module 6, the Correspondent Bank Money account is debited $50 and the money issued account is credited $50 in Step 5 (parenthetical entry). Here, $50 in electronic notes 11 are transferred through the same money module path as Steps 6-8 above, to reach the Transaction money module 4.

Figure 21 illustrates the exchange of electronic notes 11 for cash at an Issuing Bank 1. Here the subscriber has $100 of electronic notes 11 stored in his/her Transaction money module 4 and wishes to exchange $50 of the electronic notes 11 for $50 of paper cash.

After the Transaction money module 4 establishes the communications with the Issuing Bank's 1 Teller money module 5, all $100 of the electronic notes 11 is removed from the Transaction money module 4 (Step 1). This causes the Money In Transit account to be credited by $100 and the Money Due account (at the Issuing Bank 1) to be debited by $100.

The Teller money module 5 then requests $50 of updated electronic notes 11 from the Money Generator module 6, and this transaction requires the Money In Transit account to be debited by $50 and the Money Issued account to be credited by $50 (Step 2). The newly generated $50 of electronic notes 11 is then transferred to the Transaction money module 4 through the Teller money module 5. The $50 of paper cash is then transferred to the subscriber through a Teller or ATM (Steps 3-5).

Also shown in this figure (parenthetically) is the subscriber making the same exchange for cash when only $50 is stored in his/her Transaction Money Module 4. At the Issuing Bank, $50 of electronic notes 11 is removed for which the Money In Transit account is credited $50 and the Money Due account is debited $50. Fifty dollars of paper cash is then returned to the subscriber since he/she only deposited $50 of electronic notes 11 (Step 5).

Completing this transaction, in both cases the Money In Transit account is debited by $50 while the cash account at the Issuing Bank 1 is credited by $50. The net result is that the subscriber ends up with $50 of paper cash and, in the former case only, $50 of updated electronic notes 11 in his/her Transaction money module 4.

The exchange of electronic notes 11 for paper cash at a Correspondent Bank 2 is illustrated in Figure 22. As in the example illustrated in Figure 21, although the subscriber is only exchanging $50 of electronic notes 11, all $100 of electronic notes 11 are transferred from the subscriber's Transaction money module 4 (Step 1).

After the notes 11 are transferred, the Correspondent Bank's 2 Teller money module 5 credits its Money In Transit account by $100 and debits its Money Due account by $100. This $100 of electronic notes 11 is now deposited at an Issuing Bank 1, causing the Correspondent Bank 2 to credit its Money Due account by $100 while debiting its Deposited at Issuing Bank account by $100 (Step 2).

Bank 3.

The Clearing Bank 3 may be implemented in any computer processing facility capable of accommodating the large number of transactions and corresponding amounts of data which the system will typically handle. A high volume mainframe computer, a suitably sized minicomputer system, a number of networked work stations having the necessary data processing capabilities or combination of the foregoing may also be used. As will be appreciated by a person skilled in the art, the particular design of the Clearing Bank 3 hardware system is not critical to the invention.

It is anticipated that Issuing Banks 1 may clear money in one of several procedures. In one of these procedures, electronic money may be deposited on-line from the Issuing Bank 1 to the Clearing Bank 3. This could be done on-line in a real-time mode when transactions are actually occurring. Alternatively, an Issuing Bank 1 may record the details of transactions being performed during the course of the day for later batch processing. Interbank processing could occur several times a day.

As shown in Figure 26, an Issuing Bank 1 may periodically transfer its electronic money to a deposit consolidation file (consolidate deposits) which may be processed and transmitted to the Clearing Bank 3. Transaction records from this file are also conveyed to the bank's Transaction Reconciliation system 22 for statistical and housekeeping functions.

At the Clearing Bank 3, the deposit consolidation files are processed creating a single debit and credit by the monetary unit for each Issuing Bank's 1 demand account. Of course, the appropriate accounting transactions for these demand accounts are posted during the clearing processes. Any accounts which are overdrawn will be settled via the usual interbank settlement processes that are commonly used in the industry.

The processed electronic money that is cleared is sent back to the Money Issued Reconciliation System 23 of each of the banks that issued it in order to be reconciled and checked for tampering and duplication.

Additional statistical and housekeeping functions are implemented in the Money Issued Reconciliation System 23, as shown in Figure 27. Issuing Bank's 1 provide their own Money Issued Reconciliation System 23, typically embodied in a general purpose computer but not so limited, for matching the electronic money issued to the electronic money cleared at the Clearing Bank 3.

As indicated in Figure 27, the electronic money issued and electronic money deposited at Issuing Banks 1, and money cleared transactions received from clearing bank 3 are conveyed to the Money Issued Reconciliation system 23. The Money Issued Reconciliation system 23 generates accounting transactions for the money cleared, and updates a master file of all the bank's money issued. Additionally, the Money Issued Reconciliation system 23 passes to an investigation subsystem 13 money which has cleared but which was not issued or was possibly transferred more than once.

Any unmatched cases may indicate a potential breach of security. Investigators may then determine whether Money Generator modules 6 are not working properly or money modules are being tampered with. Money module identifiers of faulty or abused money modules are passed to each bank's Security Servers 27 for distribution to the other money modules on the bank's local network 18. The identifiers are also sent to the Certification Agency 28 for appropriate distribution throughout the Network 25.

Separately, the Money Issued master file is accessed by the Money Position system 24 which creates a file to be transmitted to the Clearing Bank 3 to create a consolidated money position. It is contemplated that all Issuing Banks 1 will provide a report reflecting their position at the end of a specified period, typically at the end of every day. The Money Position System 24 may consolidate these reports to reflect the amount of money issued by the Issuing Banks 1 for each monetary unit. The reports will reflect the outstanding position of each Issuing Bank 1 in order to assess the risk of interbank settlement problems.

Operational Sequences

Although some aspects of the preferred embodiment may be described in terms of detailed schematic diagrams, the transaction functions are best illustrated by use of process flowcharts. Thus, to facilitate understanding of the operation of the money modules, several examples of transactions are set forth in the flowcharts of Figures 28-50A. Referring to these figures, a detailed description of the system processes and the associated application functions that incorporate the principles of the preferred embodiment of the present invention will now be described.

Throughout the descriptions of the flowcharts (except where indicated otherwise), the application functions of the Transaction money module 4, whether they are imbedded in a hand-held unit or other type of processing device, are hereinafter designated with the suffix "A", and the Teller money module 5 applications and its associated bank are hereinafter designated with the suffix "B". In the case where a Correspondent Bank 2 interacts with an Issuing Bank 1, the Issuing or Correspondent Bank 1 and its associated Teller money module 5 applications are hereinafter designated with a "C".

Additionally, transitions to steps in another figure are indicated by a pentagonal tag having an alphanumeric symbol, and continue on the other figure with a circle having the same alphanumeric symbol therein.

modules **4,5,6** of the present embodiment. Thus, in this example, "A" denotes any class of money module.

After the bank that is to be accessed is selected, the money module initiates communication with the Network **25** under the control of its Session Manager A **31** (Step 50). The Network Server **26** begins by requesting the certificate of the Transaction money module **4** from Session Manager A **31** (Step 52-54). The Maintain Security A application **37** retrieves and sends the certificate to Session Manager A **31** (Step 56). Session Manager A **31** sends the certificate to the Network Server **26** (Step 58), which, upon receipt, routes it to the Security Server **27** (Step 60).

The Security Server **27** tests the certificate to check its validity (Step 62-64), and if it is not valid for any reason, the Security Server **27** will signal the Network Server **26** to deny access (Step 66). The Network Server **26** may in turn convey an access-denied message to Session Manager A of the Transaction money module **4** (Step 68-70).

If the Session Manager A that receives the denied access message is a Transaction money module **4**, its To Subscriber application A will inform the subscriber of this condition (Step 74). If it is a Teller money module **5** or Money Generator Module **6** that is trying to access the Network **25**, the To Bank A application **47** notifies the bank's systems **20** that its access will not be permitted (Step 76).

Assuming the certificate validity check is satisfied, the Security Server **27** sends an updated list of the bad money modules, and a new list of certificatory keys to the Session Manager A, (Step 78, Fig. 33A). The keys are signed using the last version of the certificatory key. This information is received by Session Manager A and forwarded to the Maintain Security A **37** application, which will validate the certificatory key list and the bad money module list (Steps 80-82, Fig. 33A).

Public Key A **44** tests the validity of the signature (Step 84) and if the signature is not valid, a message warning of a network security problem is sent by the To Subscriber application A **33** of a Transaction money module **4** (Steps 86-90), or alternatively, by the To Bank application A application of a Teller money module **5**, (Steps 86-88, 92). Advantageously, all money modules will check the validity of a signature received from even the Security Server **27**. This helps to ensure the integrity of the overall system.

In the case of a valid signature, Maintain Security A updates the bad money module list and the certificatory key list. (Step 94). If the certificate is to be recertified or the certificate has expired (Steps 96 and 98), the Maintain Security A generates a new certificate (Step 126 of Figure 33C) while Public Key A generates new keys and signs the certificate using the old public key (Step 128). Session Manager A sends the new certificate to the Security Server **27** who takes the certificate and tests the validity of the signature (Steps 130-136).

Assuming that the signature of the new certificate is not valid at this stage, Steps 66-76, Fig. 33, are repeated so as to terminate the communication link into the Network **25**.

On the other hand, a valid signature, Fig. 33C, will allow the Security Server **27** to sign the new certificate and send it back to the money module (Step 138). Session Manager A **31** receives the new certificate, Step 140, Fig. 33D, and forwards it to its Maintain Security application A to again validate the certificate through use of the Public Key application (Steps 142-146). Here, the money modules will repeat the test of the validity of the certificate issued from the Security Server **27**. For a valid signature, the Session Manager A **31** sends an acknowledgment to the Security Server **27** (Step 148) who responds by returning the process to Step 78, Fig. 33A.

Conversely, if the Security Server's signature on the new certificate generated by Transaction money module A proves to be invalid, Fig. 33D, Session Manager A will send an invalid certificate message along with the certificate back to the Security Server **27** (Step 150), which will again attempt to validate the signature on the certificate (Step 152). A valid signature will return the process to Step 66, Fig. 33. Alternatively, an invalid signature will cause the Security Server **27** to disconnect from the Network **25** (Step 156, Fig. 33D) and cause the Network Server **26** to notify the money module of a malfunction (Step 158).

The Session Manager A that receives the message (Step 160) will, in the case of a Transaction money module **4**, get the To Subscriber A **33** to inquire of the subscriber if they desire to retry the whole process of signing on to the Network **25** (Steps 164 & 168). In the case of a Teller money module **5** or a Money Generator Module **6**, the To Bank application A will inquire if there is a request to retry the Network **25** sign-on procedure (Steps 166 & 168).

No attempts for a retry will, of course, end the communication link into the Network **25**, and conversely, a request for retry of Network **25** access will return the procedure back to Step 56, Fig. 33, wherein Maintain Security A will again retrieve the Transaction money module's certificate for the Network Server **26**.

Back at Step 98, Fig. 33A if the certificate does not need to be recertified or has not expired, Session Manager A **31** will request the date and time (Step 100) from Clock/Timer A (Step 102, Fig. 33B), and forward this data to the Network Server **26** (Step 104).

The Network Server **26** checks the time and date after receiving it (Step 106) and if it is outside of an acceptable predetermined parameter, the Network Server **26** will send the new time and date (Step 110) to Clock/Timer A through Session Manager A (Steps 112 & 114). If Clock/Timer A **43** cannot adjust the date and time to be synchronized with the Network **25**, the operator of the money module for subscriber or the bank is notified of the clock malfunction (Steps 116-124).

In response to the apparent malfunction, the operator may attempt to have the time and date resent from the

money module involved (Step 512).

Briefly referring to Figure 37, all encrypted messages between modules will be provided by the following steps. The sending money module (here also referred to as "X") uses its Symmetric Key **45** to encode the message to be sent to the receiving money module (here also referred to as "Y"). (Step 2). Again, it will be appreciated that there are a number of known encryption techniques which may be utilized.

The Session Manager X **31** sends the encoded message to Session Manger Y **31** which in turn decodes the message using its Symmetric Key Y **45** (Steps 4-8).

Continuing with Figure 32, the Session Manager Y responds to the termination notice sent by also undoing any changes it may have made towards establishing the session, and noting the aborted session (Steps 514-516). If it is a Transaction money module **4** that is now shutting down, the To Subscriber application **33** alerts the subscriber of the condition (Step 518 & 524). Correspondingly, in a Teller money module **5**, the To Bank application **47** will reverse all accounting transactions that have been undertaken (Steps 518-522).

Returning to Figure 34B, assuming that the money module B certificate is valid, in Step 228 Maintain Security A checks to see if money module B is on the list of compromised money modules. If money module B is on the list (Step 230), the session reverts to the abort transaction procedure, Steps 500-524. Thereafter, the communications session is dissolved.

More typically, money module B will not be on the list of compromised money modules, and the Clock/Timer A **43** will retrieve the date and time (Step 232) and send this information to the Maintain Security application A **37** so that the verification message may be assembled with the date and time (Step 234).

Symmetric Key A **45** then encrypts the verification message with the date and time information, using the random session key provided by money module B (Step 236). Session Manager A **31** sends this encrypted message (Step 238) to Session Manager B **31** (Step 240). From there, the Symmetric Key application B **45** decrypts the message (Step 242) and passes it to the Maintain Security B **37** for message verification (Step 244, Fig. 34C). An incorrect message will cause the session to be aborted through Steps 500-524, while a correct message will advance the procedure so that Maintain Security B **37** can compare the time and date with that of money module A (Step 248).

Clock/Timer B **43** will verify that money module A's clock is within a preset amount of deviation from the clock of money module B (Step 250). If the discrepancy between the two clocks is greater than a predetermined amount, the session will be aborted by branching to Steps 500-524.

If there is no discrepancy that is greater than the permissible amount, Session Manager B **31** will note its start of a session (Step 252), and send an acknowledgement to money module A to start the transaction (Step 254). After the encoded message is sent from money module B to Session Manager A **31** using process steps 2-8, Fig. 37, Session Manager A **31** acknowledges the message receipt and also notes the start of session (Steps 256-258).

Request Withdrawal

After a session is established between the Transaction money module **4** and Teller money module **5**, the Transaction money module **4** makes a withdrawal request from the Teller money module **5**. See Figure 29. Referring now to Figure 30, a process for requesting a withdrawal will now be described. It should be noted that although the figure denotes the parties as "X" and "Y," in the process steps described below, they are applicable to any money module transacting with a Teller money module **5**.

To begin, the To Teller X **34** sends a withdrawal request to the Teller money module **5**, requesting a certain amount of money to be withdrawn from a specific account. In its transmission of the withdrawal request, the account number and the account profile will be transmitted from the requesting money module to the Teller money module **5** (Step 700). To send this request, the process Steps 2-8 are repeated, in which the message is encrypted using the previously described cryptographic techniques.

Validate Account Number

Once the withdrawal request and the account number and profile are transmitted to the Teller money module **5**, a procedure to validate the account number is initiated (Steps 7041-7055). A flow diagram depicting how an account number is validated is shown in Figure 38.

In this process, the Maintain Security application **37** of the Teller money module **5** receives the account profile and signature and conveys them to its Public Key application **44** to verify the profile signature (Steps 7041-7042). The signature is tested using the public key generated and distributed by the Bank's Security Server **27**. An invalid signature causes the Maintain Security **37** application to inform the Session Manager that the account profile is invalid (Step 7044), whereby Steps 500-524, Fig. 32, are followed to abort the transaction between the two money modules.

If the signature test confirms a valid signature, the procedure advances to the To Bank application **47** which sends the account number it has received on to the bank's computer systems (Step 7046). An inactive account will cause

Request Notes

Directing attention to Figure 40, notes **11** may be requested between Teller money modules **5** and Money Generator modules **6** using the following procedure described below.

The To Money Generator application **48** of the requesting Teller money module **5** will issue a request for a specific amount of electronic money to be created (Step 780). The request will be sent using the above described Steps 2-8 for encrypted transmission, to the To Teller application **34** of the Money Generator module **6** so that the Money Creator application **50** may be activated (Step 784) to create the electronic notes **11** (Step 786).

After the creation of electronic notes **11**, they are signed by the Public Key application **44** of the Money Generator module **6** (Step 788) and placed in a holder by its Notes application **40** (Step 790). Finally, the Note Directory **39** is updated with the information about the newly created electronic notes **11** (Step 792).

The process flow now returns to the procedures shown in Figure 28. The requested notes in the Money Generator module **6** are transferred to the Teller money module B **5** using the process Steps 750-770 outlined above for transferring electronic notes **11**. The notes **11** are then transferred from the Teller money module B **5** to the Transaction money module **4** using these same process Steps 750-770 for transferring- electronic notes **11**.

Finally, to successfully complete the withdrawal of electronic notes **11**, the money modules will "commit" to or finalize the transaction by utilizing the following procedure. Referring now to Figure 41 for a detailed description of this process, the Tran Log Mgr. application **36** updates its Tran Log to record the transaction that has occurred above (Step 690). When it is a Transaction money module **4** that is committing to the exchange (Step 691), the To Subscriber application will notify the subscriber that the transaction has been successfully completed (Step 692). Of course, the Session Manager application A **31** will note the end of session (Step 693), and employ process Steps 2-8 to send the message to the money module it is transacting with.

With this end of session notice received, the other money module, in this example a Teller money module **5**, will use its Tran Log Mgr. application **36** to update its own Tran Log (Step 694). Assuming, however, the second money module receiving the end of session notice is not a Teller money module **5**, an additional step of having the To Subscriber application **33** notify the subscriber of the end of the transaction occurrence (Step 696) will be necessary. Thereafter, the Session Manager **31** of the second money module in both cases will also make note of the end of the session (Step 698).

Directing attention back to Figure 28, the process to commit is initiated first by the Transaction money module **4** committing its transaction with the Teller money module B **5** (Steps 690-698). The process steps are also applied to commit the transaction between Teller money module B **5** and the Money Generator module **6** (Steps 690-698). That completes the processing for one complete withdrawal of electronic money from an Issuing Bank **1**.

Withdrawal From A Correspondent Bank

A withdrawal from a Correspondent Bank **2** will now be described, aided by reference to Figure 35. To begin, the previously described Steps 43-48 to set up a withdrawal are undertaken by a Transaction money module A **4**, in conjunction with an Teller money module B **5**. Next, Steps 190-258, used to establish a session, also described above, are initiated between Teller money module B **5** and Teller money module C **5**. After the sessions have been established, the To Bank application B **47** will post the accounting transaction corresponding to the withdrawal that is going to subsequently occur (Step 900; see also Fig. 13, Step 1).

As previously noted, it is contemplated that whenever a Transaction money module **4** interacts with a bank, both Issuing **1** and Correspondent **2**, all electronic notes **11** that are stored within the Transaction money module **4** are removed and replaced with electronic notes **11** containing the most recent certificate. To perform this operation, To Transaction B **49** will check to see if there are notes **11** stored within the Transaction money module **4** (Steps 902-904). If there are notes **11**, To Bank B **47** will post the appropriate accounting transactions (see accounting procedure illustrated in Figure 13; Step 2) (Step 906), and perform a deposit request to the Teller money module C **5** (associated with an Issuing Bank **1**) to return the notes **11** that need to be replaced.

For a detailed description for performing a deposit request, attention will be directed to Figure 44. Here, the To Teller application **34** sends a deposit request message, the amount of the deposit to be sent, the account number and the account profile of the account to which the notes **11** will be deposited (Step 920). This information is transferred to the Teller money module **5** using Steps 2-8 for sending messages, and then Steps 7041-7050 (see Figure 38) are performed to validate the account profile and number.

In the case where the depositor is a Transaction money module **4**, the To Transaction application **49** of the Teller money module **5** will send an acknowledgement to the Transaction money module **4** that the transfer of notes **11** is ready to proceed (Step 924). Alternatively, if it is another Teller money module **5** that is making the deposit, it is the To Teller application **34** that issues the acknowledgement to the Teller money module **5** (Step 926).

In either case, the acknowledgement is encrypted and transmitted using the procedure outlined in Steps 2-8,

The To Teller A **34** receives the acknowledgement (Step 430) and initiates the Steps 690-698 to commit the deposit transaction between the two money modules.

When the electronic notes **11** removed exceed the desired deposit amount, new updated notes **11** must be returned to the Transaction money module **4**. To perform this, the To Bank application B **47** of the Teller money module B **5** posts the proper accounting transactions (Step 424; Fig. 12, Step 2). Thereafter, Teller money module B **5** establishes a session with the Money Generator module **6** using process Steps 190-258, and requests electronic notes **11** from the Money Generator module **6** in the amount that should be returned to the Transaction money module **4**, by performing Steps 780-792.

The electronic notes **11** are created by the Money Generator module **6** and transferred to the Teller money module B **5** using Steps 750-770. With the electronic notes **11** in the possession of the Teller money module B **5**, they are transferred to the Transaction money module A **4** using Steps 750-770.

After Transaction money module A **4** receives the electronic notes **11**, it must finalize the transaction by committing Teller money module B **5** to Transaction money module A **4** using Steps 690-698. Likewise, Teller money module B **5** must commit to the Money Generator module **6** using the same Steps 690-698.

Deposit To A Correspondent Bank

Figure 45 illustrates the process flow for a deposit at a Correspondent Bank. In depositing to a Correspondent Bank **2**, the deposit set up described in Steps 398 through 414 are repeated in the first stage of the transaction. From there the To Transaction B **49** tests to see if the deposit is less than the total amount of electronic notes **11** that have been withdrawn in the deposit set up procedures that were just processed (Step 440).

In the case where all the electronic notes **11** stored in the Transaction money module **4** are equal to the amount of notes **11** to be deposited, then To Transaction B **49** sends a deposit acknowledgement back to the Transaction money module **4** (Step 444), using Steps 2-8 to send the message from the Teller money module B **5** to Transaction money module A **4**.

On the Transaction money module **4** side, the To Teller **34** application receives the acknowledgement (Step 446) and uses Steps 690-698 to commit the transaction with Teller money module B **5**. The Transaction money module **4** is now finished and removed from the process. The finalization of the deposit provides for the account posting transactions to be made by the To Bank application **47** (Step 448). See Figure 11, Step 1 for the accounting transactions.

A session is now established between the Teller money module B **5** and Teller money module C **5** using Steps 190-258.

Teller money module B **5** issues a request to make a deposit to the Teller money module C **5** by using process Steps 780-792. The To Bank B **47** then posts the accounting transactions (Step 450; see also Fig. 11, Step 2).

Notes **11** are now transferred from the Correspondent Bank B **2** to the Issuing Bank C **1** using Steps 750-770; the Issuing Bank C **1** posts the corresponding accounting transactions (Step 452; see also Fig. 11, Step 2). The To Teller C **34** responds by sending the deposit acknowledgement (Step 454) using Steps 2-8, to To Teller application **34** of Teller money module B **5** (Fig. 45A, Step 456).

Here again, the deposit is checked to see if it is less than the amount of electronic notes **11** that have been removed earlier, and when it is not, the withdrawal is completed with the process Steps 690-698, Fig. 41, to commit Teller money module B **5** to Teller money module C **5**.

A deposit request that is less than the amount of notes **11** that are withdrawn requires account updating (Step 460; see also Fig. 11, Step 3), and new notes **11** to replace the additional notes **11** that were taken. Accordingly, a withdrawal request following the process Steps of 700-724 from Teller money module B **5** to Teller money module C **5** is made to provide these new electronic notes **11**.

Teller money module C **5** must first establish a session with the Money Generator module **6**, using the process Steps 190-258. The new electronic notes **11** are requested by the Teller money module C **5** from the Money Generator module **6** following process Steps 780-792, which are then transferred to the Teller money module C **5** using Steps 750-770 to transfer notes **11** between money modules.

This transfer of electronic notes **11** to the Teller money module C **5** requires that accounting transactions be posted by the To Bank application C **47** (Step 462, Fig. 45B; see also Fig. 11, Step 3).

From there, the notes **11** are transferred from the Issuing Bank's **1** Teller money module C **5** to the Correspondent Bank's **2** Teller money module B **5** and to the Transaction money module **4** by using Steps 750-770 for transferring notes **11**. Thereafter, each money module must commit to the money module with which it has established a session. Thus, Transaction money module A **4** commits to Teller money module B **5**, Teller money module B **5** subsequently commits to Teller money module C **5**, which then commits to the Money Generator module **6**. All three of these commitment transactions use process Steps 690-698 above.

dissolved using abort transaction Steps 500-524.

When the funds are sufficient to meet the amount requested, the Pay/Exchange A **35** sends the amount of the dollars and the proposed dollar/pound exchange rate (Step 316) to the To Subscriber application **33** of Transaction money module B **4** using the Steps 2-8. (See Figure 46A). At this point, To Subscriber B **33** prompts Bob with the amount and rate proposed by Alice, to determine if the values are what Bob will agree to exchange (Step 322).

The Pay/Exchange B **35** receives the dollar amount and the rate that is proposed by Alice and if the amount and rate are not agreed to by Bob, Pay/Exchange B **35** will send a message indicating that the value or exchange rate is incorrect (Step 326), through the Steps of 2-8 for sending messages. To Subscriber A **33** prompts Alice for the dollar amount and exchange rate over again (Step 327). Entry of new values returns the process to Step 310 for continuation, see Fig. 46, while the lack of new values entered causes the abort transaction process of Steps 500-524 to be initiated.

If the amount and rate are agreed to by Bob, Pay/Exchange B **35** will calculate the equivalent amount in pounds, based on the rate provided (not shown), and then initiate the step of having Note Directory B **39** check to see that Transaction money module B **4** contains sufficient funds to fulfill the exchange (Step 323). When the funds in Transaction money module B **4** are insufficient to meet the exchange, Pay/Exchange B **35** sends a message to Alice of insufficient funds (Step 325) using Steps 2-8. The process flow returns to Step 327.

Proceeding with the case in which sufficient funds do exist in Transaction money module B **4**, Pay/Exchange B **35** will send an acknowledgement using Steps 2-8 to Transaction money module A **4** (Step 329). After receiving this acknowledgement, Pay/Exchange A **35** sends the amount of dollars requested to its corresponding Money Holder **38** application in Step 330. The dollars are transferred from Alice to Bob via the Steps 750-770 described above for transferring notes **11**.

Pay/Exchange B **35** receives the notes **11** and then transfers the amount of pounds to its Money Holder **38** application (Step 331). From there, the electronic pounds are transferred to Alice using the transfer notes process described in Steps 750-770. To record this exchange, Transaction money module A **4** commits with Transaction money module B **4** by using process Steps 690-698 described above. With a satisfactory exchange, the communications link between the two Transaction money modules may now be terminated.

Foreign Exchange At An Issuing Bank

Turning attention now to Figure 48, if a subscriber were to exchange his/her dollars for pounds with an Issuing Bank **1** instead of with a subscriber, the following process is followed.

Subscriber A sets up the foreign exchange transaction by signing on to his/her Transaction money module **4** (see Fig. 47Z) using Steps 10-42 described above. To Subscriber A **33** prompts the subscriber for the transaction desired (Step 334), and in this example, the subscriber chooses the dollar/pound exchange, and the amount of dollars the subscriber will exchange. It is anticipated that the choice of the bank to transact with may be an option offered to the subscriber (Step 336).

The Note Directory A **39** checks for a sufficient balance to complete the request (Step 338). An insufficient balance permits the subscriber to again enter the amount he/she will exchange (Step 340-342), whereby Session Manager A **31** will terminate the transaction (Step 345) if no new amount is entered. Entry of a new amount returns the process to Step 338 to check for sufficient funds to meet the new request. When the funds are sufficient for the exchange request, a Network **25** sign-on using Steps 50-168 is commenced.

After the Network **25** sign-on, the Network **25** checks if a bank or financial institution has been selected (Step 346). If a bank or financial institution was not chosen earlier, To Teller A **34** must prompt the Network Server **26**, through Session Manager A **31**, for a list of banks or financial institutions that will provide the exchange (Steps 348-350). The Network Server **26** sends the list (along with rates) to the subscriber through the To Teller A **34** and To Subscriber A **33** applications (Steps 352-356).

After prompting (Step 357, Fig. 47A), the subscriber chooses a bank or financial institution, or ends the transaction (Step 359). When a bank or financial institution is chosen, a session is established with the Teller money module **5** chosen using Steps 190-258 described above. After a session is established, To Teller A **34** sends the amount of dollars to be exchanged for pounds (Step 360) using Steps 2-8 for encrypting and transmitting a message.

To ensure that the subscriber still wants to proceed with the exchange, To Transaction B **49** sends the current exchange rate to the subscriber using process Steps 2-8 (Step 362). At this point, To Subscriber A **33** prompts the subscriber with the bank's exchange rate and if the subscriber does not wish to proceed, the transaction is aborted by following Steps 500-524 (Steps 364-366). If the transaction is to proceed, the dollars are transferred from Transaction money module A **4** to Teller money module B **5** using Steps 750-770 described herein.

Returning to Figure 48, once the set up of the foreign exchange transaction is accomplished, the proper accounting transactions are posted (Step 368; also illustrated in Figure 15, Step **1**) to reflect the dollars that have just been transferred. A session is established between Teller money module B **5** and a Money Generator module **6** via Steps 190-258. Teller money module B **5** requests the proper pound notes **11** through process Steps 780-792. The notes **11** are returned

etary systems.

Operation of the invention has been described primarily with currency notes and credit notes that can be used by subscribers in the same processes. It will be understood that the described system can also be adapted to other monetary instruments. For example, personal and corporate checks and bank drafts could be provided by enhancing several of the Transactor applications. More complicated multiparty payment processes such as letters of credit and banker's acceptances could also be provided with appropriate changes to the system. It may also be possible to adapt the system of the invention to provide corporate financial obligations such as commercial paper.

Moreover, although the invention has been described in detail with particular reference to a preferred embodiment thereof, it should be understood that the invention is capable of other and different embodiments, and its details are capable of modifications in various obvious respects. As is readily apparent to those skilled in the art, variations and modifications can be affected while remaining within the scope of the appended claims. Accordingly, the foregoing disclosure, description, and figures are for illustrative purposes only, and do not in any way limit the invention, which is defined only by the claims.

Claims

1. An electronic monetary system comprising

   a computer controlled accounting system associated with an issuing bank (1);
   a money generator module (6) associated with said issuing bank (1), that generates electronic representations of currency (11), wherein a money issued liability account in said accounting system is credited by an amount associated with generated electronic representations of currency;
   a teller module (5) associated with said issuing bank (1), capable of storing said electronic representations of currency (11), and intermediating banking transactions involving said electronic representations of currency (11);
   a transaction module (4) capable of storing said electronic representations of currency (11), performing on-line transactions with said teller module (5), and exchanging said electronic representations of currency (11) with other transaction modules (4) in off-line transactions;
   where said electronic representations of currency (11) each include an original monetary value generated by said money generator module (6), a transferred monetary value, and a module identifier that designates the module which has received said electronic representation of currency; and
   said teller and transaction modules (5, 4) having processors operative, when said modules (5, 4) are functioning as transferor modules transferring one of said electronic representations of currency (11) to a transferee module, to generate a transfer record having said transferred monetary value and said transferee module identifier and to include said transfer record and said initial monetary value in said transferred electronic representation of currency.

2. The electronic monetary system of claim 1, characterized in that said money generator module (6) and said teller module (5) are embodied in a device having a single processor.

3. The electronic monetary system of claim 1, characterized in that said transaction module (4) and said teller module (5) each have a note directory (39) for keeping track of a current monetary value for each of said electronic representations of currency (11) stored therein.

4. The electronic monetary system of claim 3, characterized in that said current monetary value recorded in said note directory (39) of said transferor module, and associated with one of said electronic representations of currency (11) stored therein, is decremented by said transferred monetary value upon transferring said transferred electronic representation of currency (11) to said transferee module.

5. The electronic monetary system of claim 1, characterized in that said electronic representations of currency (11) include a money generator digital signature produced by said money generator (6) and a transferor digital signature produced by said transferor module.

6. The electronic monetary system of claim 5, characterized in that said electronic representations of currency (11) include certificates corresponding to said money generator digital signature, and said transferor digital signature, where each of said certificates includes a module identifier and a first cryptographic key of said digital signature producer, and where said first cryptographic key is used to validate said corresponding digital signature.

said teller module (5), said money generator module (6) generating a new replacement electronic representation of currency (11) having a new expiration date, and said teller module (5) transferring said new replacement electronic representation of currency (11) to said transaction module (4).

20. The electronic monetary system of claim 14, characterized in that said money generator, teller, and transaction modules (4) are tamper-proof devices that are capable of communicating via cryptographically secure sessions.

21. The electronic monetary system of claim 20, characterized in that each said module may commit by logging a transaction so that it can no longer abort said transaction by rolling-back its state; and wherein each said module may abort during said transaction by following a programmed abort routine, where control is transferred to said abort routine from other routines or a time-out protocol.

22. An electronic monetary system comprising

a computer controlled accounting system associated with an issuing bank (1);
a money generator module (6) associated with said issuing bank (1), that generates electronic representations of currency (11), wherein a money issued liability account in said accounting system is credited by an amount associated with generated electronic representations of currency;
a teller module (5) associated with said issuing bank (1), capable of storing said electronic representations of currency (11), and intermediating banking transactions involving said electronic representations of currency (11);
a transaction module (4) capable of storing said electronic representations of currency (11), performing on-line transactions with said teller module (5), and exchanging said electronic representations of currency (11) with other transaction modules (4) in off-line transactions;
a security server (27) used for implementing the security of the electronic monetary system;
where said money generator module (6), said teller module (5), and said transaction module (4) are each associated with a unique module identifier contained within a certificate that is digitally signed by said security server (27), where said certificates are only valid for a limited period of time, after which time said associated module will not be able to transact with other modules until a new certificate is obtained;
wherein said new certificate and compromised module identifiers are obtained when said module performs initial network connection to a network having one or more security servers;
wherein said module will not transact with any other module having one of said compromised module identifiers.

23. The electronic monetary system of claim 22, characterized in that said money generator module (6) and said teller module (5) are embodied in a device having a single processor.

24. The electronic monetary system of claim 22, characterized in that said accounting system maintains money due and money in transit accounts during deposits and withdrawals of said electronic representations of currency (11).

25. The electronic monetary system of claim 22, characterized in that said security server (27) distributes a certificatory key, when required.

26. The electronic monetary system of claim 22, characterized in that said security server (27) digitally signs an account profile having data fields including a bank identifier, an account number, and an indication of account type, where said account profile is used by said transaction module (4) to access a subscriber account identified by said account number.

27. The electronic monetary system of claim 22, characterized in that said money generator module (6), teller module (5), transaction module (4), and security server (27) are tamper-proof devices capable of communicating via cryptographically secure sessions.

28. The electronic monetary system of claim 27, characterized in that each said module and said security server (27) may commit by logging a transaction so that it can no longer abort said transaction by rolling-back its state; and wherein each said module and said security server (27) may abort during said transaction by following a programmed abort routine, where control is transferred to said abort routine from other routines or a time-out protocol.

29. An electronic monetary system comprising

a transaction module (4) that stores said electronic representations of currency (11), performs on-line transactions with said plurality of second teller modules (5), and exchanges said electronic representations of currency (11) with other transaction modules (4) in off-line transactions;
where said first teller module (5) has a first processor that intermediates transactions among said first accounting system, said money generator module (6), and said second teller module (5); and
where said second teller module (5) has a second processor that intermediates transactions among said second accounting system, said first teller module (5), and said transaction module (4).

38. The electronic monetary system of claim 37, characterized in that said transaction module (4) also performs on-line transactions with said teller module (5), and wherein said first teller module (5) also intermediates transactions involving said transaction module (4).

39. The electronic monetary system of claim 37, characterized in that said money generator module (6) and said first teller module (5) are embodied in an electronic processing device controlled by said first processor.

40. The electronic monetary system of claim 37, characterized in that said first and second accounting systems maintain money due and money in transit accounts during deposits and withdrawals of said electronic representations of currency (11).

41. The electronic monetary system of claim 37, characterized in that said money generator, transaction, and teller modules (6, 4, 5) are tamper-proof devices capable of communicating via cryptographically secure sessions.

42. The electronic monetary system of claim 41, characterized in that each said module may commit by logging a transaction so that it can no longer abort said transaction by rolling-back its state; and wherein each said module may abort during said transaction by following a programmed abort routine, where control is transferred to said abort routine from other routines or a time-out protocol.

43. An electronic monetary system comprising

a plurality of computer controlled accounting systems associated with a plurality of issuing banks (1);
a plurality of money generator modules (6) associated with said plurality of issuing banks, that generate electronic representations of currency (11), wherein money issued liability accounts in said accounting systems are credited by amounts associated with generated electronic representations of currency;
a plurality of teller modules (5) associated with said plurality of issuing banks (1), capable of storing said electronic representations of currency (11);
a data processing system associated with a clearing bank, that clears said electronic representations of currency and maintains a clearing bank accounting system in which said plurality of issuing banks each has an account;
where each of said electronic representations of currency (11) includes an issuing bank identifier; and
where each of said plurality of teller modules (5) sends electronic representations of currency (11) deposited at its issuing bank (1) but issued by another issuing bank (1) to said clearing bank (3) for balancing said issuing bank accounts and for sending each said electronic representation of currency (11) back to said issuing bank (1) indicated by its issuing bank identifier.

44. The electronic monetary system of claim 43, characterized in that at least one of said money generator modules (6) and one of said teller modules (5) are embodied in a device having a single processor.

45. The electronic monetary system of claim 43, characterized in that said accounting systems maintain money in transit and money due accounts during clearing of said electronic representations of currency (11).

46. The electronic monetary system of claim 43, characterized in that said money generator modules (6) and said teller modules (5) are tamper-proof devices capable of communicating via cryptographically secure sessions.

47. The electronic monetary system of claim 46, characterized in that each said module may commit by logging a transaction so that it can no longer abort said transaction by rolling-back its state; and wherein each said module may abort during said transaction by following a programmed abort routine, where control is transferred to said abort routine from other routines or a time-out protocol.

48. An electronic monetary system comprising

a plurality of computer controlled accounting systems associated with a plurality of issuing banks (1);
a plurality of money generator modules (6) associated with said plurality of issuing banks, that generate electronic credit authorizations (11), wherein credit lines of subscriber's loan accounts in said accounting systems are drawn upon by amounts associated with generated electronic credit authorizations;
a plurality of teller modules (5) associated with said plurality of issuing banks (1), capable of storing said electronic credit authorizations (11);
a data processing system associated with a clearing bank, that clears said electronic credit authorizations and maintains a clearing bank accounting system in which said plurality of issuing banks each has an account;
where each of said electronic credit authorizations (11) includes an issuing bank identifier; and
where each of said plurality of teller modules (5) sends electronic credit authorizations (11) deposited at its issuing bank (1) but issued by another issuing bank (1) to said clearing bank (3) for balancing said issuing bank accounts and for sending each said electronic credit authorization (11) back to said issuing bank (1) indicated by its issuing bank identifier.

49. The electronic monetary system of claim 48, characterized in that at least one of said money generator modules (6) and one of said teller modules (5) are embodied in a device having a single processor.

50. The electronic monetary system of claim 48, characterized in that said accounting systems maintain money in transit and money due accounts during clearing of said electronic credit authorizations (11).

51. The electronic monetary system of claim 48, characterized in that said money generator modules (6) and said teller modules (5) are tamper-proof devices capable of communicating via cryptographically secure sessions.

52. The electronic monetary system of claim 51, characterized in that each said module may commit by logging a transaction so that it can no longer abort said transaction by rolling-back its state; and wherein each said module may abort during said transaction by following a programmed abort routine, where control is transferred to said abort routine from other routines or a time-out protocol.

53. An electronic monetary system comprising

a computer controlled accounting system and a computer implemented money issued reconciliation system (23) associated with an issuing bank (1);
a money generator module associated with said issuing bank, that generates electronic representations of money (11) that are accounted for in said accounting system;
a teller module (5) associated with said issuing bank (1), capable of storing said electronic representations of money (11);
where said electronic representations of money (11) include a note identifier used to uniquely identify each said electronic representation of money (11), and a list of transfer records to provide value subdividability of each said electronic representaiton of money;
where said money issued reconciliation system (23) maintains a record, derived from said money generator module, of said electronic representations of money (11) that issued from said issuing bank (1); and
where electronic representations of money (11) that are deposited are sent to said money issued reconciliation system (23) having a processor for matching said record of electronic representations of money (11) that issued to those subdivided electronic representations of money (11) deposited; and
where unmatched cases may indicate note counterfeiting in said electronic monetary system.

54. The electronic monetary system of claim 53, characterized in that said money generator module (6) and said teller module (5) are embodied in a device having a single processor.

55. The electronic monetary system of claim 53, characterized in that each said module may commit by logging a transaction so that it can no longer abort said transaction by rolling-back its state; and wherein each said module may abort during said transaction by following a programmed abort routine, where control is transferred to said abort routine from other routines or a time-out protocol.

56. An electronic monetary system comprising

a computer controlled accounting system and a computer implemented transaction reconciliation system (22) associated with an issuing bank (1);
a money generator module associated with said issuing bank, that generates electronic representations of money that are accounted for in said accounting system;
a teller module (5) associated with said issuing bank (1), capable of storing said electronic representations of money (11);
where transaction records from said money generator module (6), said teller module (5), and said on-line accounting system are periodically passed to said transaction reconciliation system (22);
said transaction reconciliation system (22) having a processor for analyzing said transaction records to ensure that teller transactions match the appropriate accounting transactions and to ensure that money generator module transactions match the appropriate teller transactions and accounting transactions; and
where any mismatches may indicate incomplete processing or a security breach.

57. The electronic monetary system of claim 56, characterized in that said money generator module (6) and said teller module (5) are embodied in a device having a single processor.

58. The electronic monetary system of claim 56, characterized in that each said module may commit by logging a transaction so that it can no longer abort said transaction by rolling-back its state; and wherein each said module may abort during said transaction by following a programmed abort routine, where control is transferred to said abort routine from other routines or a time-out protocol.

Patentansprüche

1. Elektronisches Zahlungsverkehrsystem, das folgendes umfaßt:

ein computergesteuertes Abrechnungssystem, das einer Emissionsbank (1) zugeordnet ist;
ein der genannten Emissionsbank (1) zugeordnetes Geldgeneratormodul (6), das elektronische Darstellungen von Geld (11) erzeugt, wobei auf einem Geldemissions-Passivkonto in dem genannten Abrechnungssystem ein Betrag gutgeschrieben wird, der den erzeugten elektronischen Darstellungen von Geld zugeordnet ist;
ein der genannten Emissionsbank (1) zugeordnetes Terminalmodul (5), das die genannten elektronischen Darstellungen von Geld (11) speichern kann, und das bei Banktransaktionen, die die genannten elektronischen Darstellungen von Geld (11) aufweisen, Intermediärfunktionen ausführt;
ein Transaktionsmodul (4), das die genannten elektronischen Darstellungen von Geld (11) speichern kann, wobei das Modul ferner Online-Transaktionen mit dem genannten Terminalmodul (5) ausführen und die genannten elektronischen Darstellungen von Geld (11) in Offline-Transaktionen mit anderen Transaktionsmodulen (4) austauschen kann;
wobei die genannten elektronischen Darstellungen von Geld (11) jeweils einen von dem genannten Geldgeneratormodul (6) erzeugten ursprünglichen Geldwert, einen übermittelten Geldwert und einen Modulidentifizierer aufweisen, der das Modul bezeichnet, das die genannte elektronische Darstellung von Geld empfangen hat; und
wobei die genannten Terminal- und Transaktionsmodule (5, 4) Prozessoren aufweisen, die bei einer Funktion der genannten Module (5, 4) als Übertragungsmodule, die eine der genannten elektronischen Darstellungen von Geld (11) zu einem Empfängermodul übertragen, derart funktionsfähig sind, daß sie einen Übertragungsdatensatz erzeugen, der den genannten übertragenen Geldwert und den genannten Empfängermodulidentifizierer aufweist, und wobei der genannte Übertragungsdatensatz und der genannte ursprüngliche Geldwert in der genannten elektronischen Darstellung von Geld enthalten sind.

2. Elektronisches Zahlungsverkehrsystem nach Anspruch 1, dadurch gekennzeichnet, daß das genannte Geldgeneratormodul (6) und das genannte Terminalmodul (5) in einer Vorrichtung mit einem einzigen Prozessor vorgesehen sind.

3. Elektronisches Zahlungsverkehrsystem nach Anspruch 1, dadurch gekennzeichnet, daß das genannte Transaktionsmodul (4) und das genannte Terminalmodul (5) jeweils ein Notenverzeichnis (39) aufweisen, um einen aktuellen Geldwert für jede der darin gespeicherten genannten elektronischen Darstellungen von Geld (11) aufzuzeichnen.

4. Elektronisches Zahlungsverkehrsystem nach Anspruch 3, dadurch gekennzeichnet, daß der in dem genannten

Notenverzeichnis (39) des genannten Übertragungsmoduls gespeicherte aktuelle Geldwert, der einem der darin gespeicherten elektronischen Darstellungen von Geld (11) zugeordnet ist, nach der Übertragung der genannten elektronischen Darstellung von Geld (11) zu dem genannten Empfängermodul durch den genannten übertragenen Geldwert vermindert wird.

5. Elektronisches Zahlungsverkehrsystem nach Anspruch 1, dadurch gekennzeichnet, daß die genannten elektronischen Darstellungen von Geld (11) eine von dem genannten Geldgenerator (6) erzeugte digitale Geldgeneratorunterschrift sowie eine von dem genannten Übertragungsmodul erzeugte digitale Übertragungsunterschrift aufweisen.

6. Elektronisches Zahlungsverkehrsystem nach Anspruch 5, dadurch gekennzeichnet, daß die genannten elektronischen Darstellungen von Geld (11) Bestätigungsvermerke aufweisen, die der genannten digitalen Geldgeneratorunterschrift und der genannten digitalen Übertragungsunterschrift entsprechen, wobei jeder der genannten Bestätigungsvermerke einen Modulidentifizierer sowie einen ersten kryptographischen Schlüssel des Erzeugers der genannten digitalen Unterschrift aufweist, und wobei der genannte erste kryptographische Schlüssel zur Bestätigung bzw. zur Validierung der genannten entsprechenden digitalen Unterschrift verwendet wird.

7. Elektronisches Zahlungsverkehrsystem nach Anspruch 6, dadurch gekennzeichnet, daß die genannten Bestätigungsvermerke von einem Sicherheits-Server (27) digital unterschrieben werden, der einer Bestätigungsvertretungseinrichtung zugeordnet ist, und wobei die genannten Bestätigungsvermerke unter Verwendung eines zweiten kryptographischen Schlüssels des genannten Sicherheits-Servers (27) bestätigt werden können, der für das genannte Terminalmodul (5) und für das genannte Übertragungsmodul (4) verfügbar ist.

8. Elektronisches Zahlungsverkehrsystem nach Anspruch 1, dadurch gekennzeichnet, daß der genannte Übertragungsdatensatz ferner das Übertragungs- bzw. das Überweisungsdatum anzeigt.

9. Elektronisches Zahlungsverkehrsystem nach Anspruch 1, dadurch gekennzeichnet, daß die genannten elektronischen Darstellungen von Geld (11) eine Liste von Übertragungsdatensätzen aufweisen, die jeweils einen Empfängermodulidentifizierer aufweisen.

10. Elektronisches Zahlungsverkehrsystem nach Anspruch 9, dadurch gekennzeichnet, daß das genannte Empfängermodul bestätigt, daß der letzte Übertragungsdatensatz in der genannten übertragenen elektronischen Darstellung von Geld (11) einen Empfängermodulidentifizierer aufweist, der einem Modulidentifizierer des genannten Übertragungsmoduls entspricht.

11. Elektronisches Zahlungsverkehrsystem nach Anspruch 1, dadurch gekennzeichnet, daß es sich bei den genannten Geldgenerator-, Terminal- und Transaktionsmodulen (6, 5, 4) um eingriffsichere Vorrichtungen handelt, die über kryptographisch sichere Sitzungen kommunikationsfähig sind.

12. Elektronisches Zahlungsverkehrsystem nach Anspruch 11, dadurch gekennzeichnet, daß jedes der genannten Module (6, 5, 4) so konfiguriert ist, daß es als ein modularer Coprozessor einer elektronischen Verarbeitungsvorrichtung funktionsfähig ist.

13. Elektronisches Zahlungsverkehrsystem nach Anspruch 11, dadurch gekennzeichnet, daß sich jedes der genannten Module (6, 5, 4) durch Protokollierung einer Transaktion verpflichten kann, so daß kein Abbruch der genannten Transaktion durch Wiederherstellung des Zustands durchgeführt werden kann; und wobei jedes der genannten Module während der genannten Transaktion durch Befolgen einer programmierten Abbruchroutine einen Abbruch durchführen kann, wobei die Steuerung von anderen Routinen oder einem Unterbrechungsprotokoll übertragen wird.

14. Elektronisches Zahlungsverkehrsystem, das folgendes umfaßt:

ein computergesteuertes Abrechnungssystem, das einer Emissionsbank (1) zugeordnet ist;
ein der genannten Emissionsbank (1) zugeordnetes Geldgeneratormodul (6), das elektronische Darstellungen von Geld (11) erzeugt, wobei auf einem Geldemissions-Passivkonto in dem genannten Abrechnungssystem ein Betrag gutgeschrieben wird, der den erzeugten elektronischen Darstellungen von Geld zugeordnet ist;
ein der genannten Emissionsbank (1) zugeordnetes Terminalmodul (5), das die genannten elektronischen Darstellungen von Geld (11) speichern kann, und das bei Banktransaktionen, die die genannten elektronischen

Darstellungen von Geld (11) aufweisen, Intermediärfunktionen ausführt;
ein Transaktionsmodul (4), das die genannten elektronischen Darstellungen von Geld (11) speichern kann, wobei das Modul ferner Online-Transaktionen mit dem genannten Terminalmodul (5) ausführen und die genannten elektronischen Darstellungen von Geld (11) in Offline-Transaktionen mit anderen Transaktionsmodulen (4) austauschen kann;
wobei die genannten elektronischen Darstellungen von Geld (11) ein Verfallsdatum aufweisen;
wobei die genannten anderen Transaktionsmodule (4) Prozessoren aufweisen, die die Annahme versuchter Übertragungen der genannten elektronischen Darstellungen von Geld (11) abweisen können, wenn die genannten versuchten Übertragungen nach dem Verfallsdatum der genannten elektronischen Darstellungen von Geld (11) auftreten.

15. Elektronisches Zahlungsverkehrsystem nach Anspruch 14, dadurch gekennzeichnet, daß das genannte Geldgeneratormodul (6) und das genannte Terminalmodul (5) in einer Vorrichtung mit einem einzigen Prozessor vorgesehen sind.

16. Elektronisches Zahlungsverkehrsystem nach Anspruch 14, dadurch gekennzeichnet, daß das genannte Abrechnungssystem während Einzahlungen und Auszahlungen der genannten elektronischen Darstellungen von Geld (11) Forderungskonten und Duchgangskonten führt.

17. Elektronisches Zahlungsverkehrsystem nach Anspruch 14, dadurch gekennzeichnet, daß das genannte Verfallsdatum abhängig von einem Geldwert variiert, der den genannten elektronischen Darstellungen von Geld (11) zugeordnet ist.

18. Elektronisches Zahlungsverkehrsystem nach Anspruch 14, dadurch gekennzeichnet, daß die in dem genannten Transaktionsmodul (4) gespeicherten elektronischen Darstellungen von Geld (11) aktualisiert werden, wenn eine Transaktion mit dem genannten Terminalmodul (5) durchgeführt wird.

19. Elektronisches Zahlungsverkehrsystem nach Anspruch 18, dadurch gekennzeichnet, daß die genannten elektronischen Darstellungen von Geld (11) von dem genannten Transaktionsmodul (4) aktualisiert werden, die die genannten gespeicherten elektronischen Darstellungen von Geld (11) zu dem genannten Terminalmodul (5) übertragen, wobei das genannte Geldgeneratormodul (6) eine neue ersetzende elektronische Darstellung von Geld (11) erzeugt, die ein neues Verfallsdatum aufweist, und wobei das genannte Terminalmodul (5) die genannte neue ersetzende elektronische Darstellung von Geld (11) zu dem genannten Transaktionsmodul (4) überträgt.

20. Elektronisches Zahlungsverkehrsystem nach Anspruch 14, dadurch gekennzeichnet, daß es sich bei den genannten Geldgenerator-, Terminal- und Transaktionsmodulen (4) um eingriffsichere Vorrichtungen handelt, die über kryptographisch sichere Sitzungen kommunikationsfähig sind.

21. Elektronisches Zahlungsverkehrsystem nach Anspruch 20, dadurch gekennzeichnet, daß sich jedes der genannten Module durch Protokollierung einer Transaktion verpflichten kann, so daß kein Abbruch der genannten Transaktion durch Wiederherstellung des Zustands durchgeführt werden kann; und wobei jedes der genannten Module während der genannten Transaktion durch Befolgen einer programmierten Abbruchroutine einen Abbruch durchführen kann, wobei die Steuerung von anderen Routinen oder einem Unterbrechungsprotokoll übertragen wird.

22. Elektronisches Zahlungsverkehrsystem, das folgendes umfaßt:

ein computergesteuertes Abrechnungssystem, das einer Emissionsbank (1) zugeordnet ist;
ein der genannten Emissionsbank (1) zugeordnetes Geldgeneratormodul (6), das elektronische Darstellungen von Geld (11) erzeugt, wobei auf einem Geldemissions-Passivkonto in dem genannten Abrechnungssystem ein Betrag gutgeschrieben wird, der den erzeugten elektronischen Darstellungen von Geld zugeordnet ist;
ein der genannten Emissionsbank (1) zugeordnetes Terminalmodul (5), das die genannten elektronischen Darstellungen von Geld (11) speichern kann, und das bei Banktransaktionen, die die genannten elektronischen Darstellungen von Geld (11) aufweisen, Intermediärfunktionen ausführt;
ein Transaktionsmodul (4), das die genannten elektronischen Darstellungen von Geld (11) speichern kann, wobei das Modul ferner Online-Transaktionen mit dem genannten Terminalmodul (5) ausführen und die genannten elektronischen Darstellungen von Geld (11) in Offline-Transaktionen mit anderen Transaktionsmodulen (4) austauschen kann;
einen Sicherheits-Server (27), der zur Realisierung der Sicherheit des elektronischen Zahlungsverkehrsy-

stems verwendet wird;
wobei das genannte Geldgeneratormodul (6), das genannte Terminalmodul (5) und das genannte Transaktionsmodul (4) jeweils einem eindeutigen Modulidentifizierer zugeordnet sind, der sich in einem Bestätigungsvermerk befindet, der eine digitale Unterschrift des genannten Sicherheits-Servers (27) trägt, wobei die genannten Bestätigungsvermerke nur über einen begrenzten Zeitraum Gültigkeit haben, wobei das genannte zugeordnete Modul nach Ablauf dieses Zeitraums nicht mehr in der Lage ist mit anderen Modulen Transaktionen durchzuführen, bis ein neuer Bestätigungsvermerk vorgesehen wird;
wobei der genannte neue Bestätigungsvermerk und die beinhalteten Modulidentifizierer vorgesehen werden, wenn das genannte Modul eine erste Netzverbindung mit einem Netzwerk herstellt, das einen oder mehrere Sicherheits-Server aufweist;
wobei das genannte Modul mit keinem anderen Modul in Transaktion tritt, das einen der genannten beinhalteten Modulidentifizierer aufweist.

23. Elektronisches Zahlungsverkehrsystem nach Anspruch 22, dadurch gekennzeichnet, daß das genannte Geldgeneratormodul (6) und das genannte Terminalmodul (5) in einer Vorrichtung mit einem einzigen Prozessor vorgesehen sind.

24. Elektronisches Zahlungsverkehrsystem nach Anspruch 22, dadurch gekennzeichnet, daß das genannte Abrechnungssystem während Einzahlungen und Auszahlungen der genannten elektronischen Darstellungen von Geld (11) Forderungskonten und Duchgangskonten führt.

25. Elektronisches Zahlungsverkehrsystem nach Anspruch 22, dadurch gekennzeichnet, daß der genannte Sicherheits-Server (27) einen bestätigenden Schlüssel verteilt, falls dies erforderlich ist.

26. Elektronisches Zahlungsverkehrsystem nach Anspruch 22, dadurch gekennzeichnet, daß der genannte Sicherheits-Server (27) ein Kontenprofil digital unterzeichnet, das Datenfelder aufweist, die einen Bankenidentifizierer, eine Kontonummer und eine Indikation der Kontenart aufweisen, wobei das genannte Kontenprofil von dem genannten Transaktionsmodul (4) dazu verwendet wird, um auf ein durch die genannte Kontonummer identifiziertes Teilnehmerkonto zuzugreifen.

27. Elektronisches Zahlungsverkehrsystem nach Anspruch 22, dadurch gekennzeichnet, daß es sich bei dem genannten Geldgeneratormodul (6), dem Tellermodul (5), dem Transaktionsmodul (4) und dem Sicherheits-Server (27) um eingriffsichere Vorrichtungen handelt, die über kryptographisch sichere Sitzungen kommunikationsfähig sind.

28. Elektronisches Zahlungsverkehrsystem nach Anspruch 27, dadurch gekennzeichnet, daß sich jedes der genannten Module und der genannte Sicherheits-Server (27) durch Protokollierung einer Transaktion verpflichten können, so daß kein Abbruch der genannten Transaktion durch Wiederherstellung des Zustands durchgeführt werden kann; und wobei jedes der genannten Module und der genannte Sicherheits-Server (27) während der genannten Transaktion durch Befolgen einer programmierten Abbruchroutine einen Abbruch durchführen können, wobei die Steuerung von anderen Routinen oder einem Unterbrechungsprotokoll übertragen wird.

29. Elektronisches Zahlungsverkehrsystem, das folgendes umfaßt:

ein computergesteuertes Abrechnungssystem, das einer Emissionsbank (1) zugeordnet ist;
ein der genannten Emissionsbank zugeordnetes Geldgeneratormodul (6), das elektronische Kreditzusagen (11) erzeugen, wobei ein Kreditrahmen eines Teilnehmer-Darlehenskontos in dem genannten Abrechnungssystem um einen Betrag in Anspruch genommen wird, der den genannten erzeugten elektronischen Kreditzusagen entspricht;
ein der genannten Emissionsbank (1) zugeordnetes Terminalmodul (5), das die genannte elektronische Kreditzusage (11) speichern kann und das Banktransaktionen, die die genannten elektronischen Kreditzusagen (11) aufweisen, Intermediärfunktionen ausführt;
ein Transaktionsmodul (4), das die genannten elektronischen Kreditzusagen (11) speichern, Online-Transaktionen mit dem genannten Terminalmodul (5) durchführen sowie die genannte elektronische Kreditzusage (11) in einer Offline-Transaktion zu einem anderen Transaktionsmodul (4) übertragen kann; und
wobei die genannte elektronische Kreditzusage (11) eine Kontonummer des genannten Teilnehmer-Darlehenskontos, einen ursprünglichen Geldbetrag und eine von dem genannten Geldgeneratormodul (6) erzeugte digitale Unterschrift aufweist;
wobei die genannte elektronische Kreditzusage zwischen Transaktionsmodulen in einem Übertragungsgeld-

betrag übertragen werden kann, der kleiner oder gleich dem genannten ursprünglichen Geldbetrag ist; und wobei die genannte Emissionsbank (1) bei Einzahlung der genannten elektronischen Kreditzusage (11) das genannte Teilnehmer-Darlehenskonto mit dem genannten übertragenen Geldbetrag belastet.

30. Elektronisches Zahlungsverkehrsystem nach Anspruch 29, dadurch gekennzeichnet, daß das genannte Geldgeneratormodul (6) und das genannte Terminalmodul (5) in einer Vorrichtung mit einem einzigen Prozessor vorgesehen sind.

31. Elektronisches Zahlungsverkehrsystem nach Anspruch 29, dadurch gekennzeichnet, daß das genannte Abrechnungssystem während Einzahlungen und Auszahlungen der genannten elektronischen Kreditzusage (11) Forderungskonten und Duchgangskonten führt.

32. Elektronisches Zahlungsverkehrsystem nach Anspruch 29, dadurch gekennzeichnet, daß das genannte Transaktionsmodul (4) nur einmal die genannte elektronische Kreditzusage (11) zu einem anderen Transaktionsmodul (4) übertragen kann.

33. Elektronisches Zahlungsverkehrsystem nach Anspruch 29, dadurch gekennzeichnet, daß es sich bei dem genannten Geldgenerator, den Terminal- und Transaktionsmodulen (4) um eingriffsichere Vorrichtungen handelt, die über kryptographisch sichere Sitzungen kommunikationsfähig sind.

34. Elektronisches Zahlungsverkehrsystem nach Anspruch 33, dadurch gekennzeichnet, daß die genannte elektronische Kreditzusage (11) digitale Unterschriften aufweist, die von den genannten Terminal- und Transaktionsmodulen (5, 4) nach der Übertragung der genannten elektronischen Kreditzusage (11) erzeugt werden; und wobei das genannte Geldgeneratormodul (6), das genannte Terminalmodul (5) und das genannte Transaktionsmodul (4) jeweils einem elektronischen Bestätigungsvermerk zugeordnet sind, durch den andere Module ihre Authentizität bestätigen können; wobei die genannte Übertragung der genannten elektronischen Kreditzusage (11) von dem genannten Transaktionsmodul (4) zu dem genannten anderen Transaktionsmodul (4) ohne Teilnehmeridentifizierung durchgeführt werden kann.

35. Elektronisches Zahlungsverkehrsystem nach Anspruch 33, dadurch gekennzeichnet, daß sich jedes der genannten Module durch Protokollierung einer Transaktion verpflichten kann, so daß kein Abbruch der genannten Transaktion durch Wiederherstellung des Zustands durchgeführt werden kann; und wobei jedes der genannten Module während der genannten Transaktion durch Befolgen einer programmierten Abbruchroutine einen Abbruch durchführen kann, wobei die Steuerung von anderen Routinen oder einem Unterbrechungsprotokoll übertragen wird.

36. Elektronisches Zahlungsverkehrsystem nach Anspruch 29, dadurch gekennzeichnet, daß das genannte Transaktionsmodul (4) sowohl elektronische Darstellungen von Geld (11) als auch elektronische Kreditzusagen (11) speichern kann, und wobei das genannte Transaktionsmodul (4) sowohl die genannten elektronischen Darstellungen von Geld (11) als auch die genannten elektronischen Kreditzusagen (11) über eine kryptographisch sichere Sitzung in einer einzigen Transaktionsübertragung zu dem genannten anderen Transaktionsmodul (4) übertragen kann.

37. Elektronisches Zahlungsverkehrsystem, das folgendes umfaßt:

ein erstes computergesteuertes Abrechnungssystem, das einer Emissionsbank (1) zugeordnet ist;
ein der genannten Emissionsbank (1) zugeordnetes Geldgeneratormodul, das elektronische Darstellungen von Geld (11) erzeugt, wobei auf einem Geldemissions-Passivkonto in dem genannten Abrechnungssystem ein Betrag gutgeschrieben wird, der den erzeugten elektronischen Darstellungen von Geld zugeordnet ist;
ein der genannten Emissionsbank (1) zugeordnetes erstes Terminalmodul (5), das die genannten elektronischen Darstellungen von Geld (11) speichern kann;
eine Mehrzahl zweiter computergesteuerter Abrechnungssysteme, die jeweils einer entsprechenden Bank (2) zugeordnet sind, wobei jede entsprechende Bank ein Konto in dem genannten ersten Abrechnungssystem führt;
eine Mehrzahl zweiter Terminalmodule (5), die jeweils einer der entsprechenden Banken (2) zugeordnet sind, wobei die Module jeweils die genannten elektronischen Darstellungen von Geld (11) speichern können;
ein Transaktionsmodul (4), das die genannten elektronischen Darstellungen von Geld (4) speichert, Online-Transaktionen mit der genannten Mehrzahl zweiter Terminalmodule (5) durchführt sowie Austauschoperationen der genannten elektronischen Darstellungen von Geld (11) mit anderen Transaktionsmodulen (4) in Offline-Transaktionen;

wobei das genannte erste Terminalmodul (5) einen ersten Prozessor aufweist, der bei Transaktionen zwischen dem genannten ersten Abrechnungssystem, dem genannten Geldgeneratormodul (6) und dem genannten zweiten Terminalmodul (5) Intermediärfunktionen ausführt; und
wobei das genannte zweite Terminalmodul (5) einen zweiten Prozessor aufweist, der bei Transaktionen zwischen dem genannten zweiten Abrechnungssystem, dem genannten ersten Terminalmodul (5) und dem genannten Transaktionsmodul (4) Intermediärfunktionen ausführt.

38. Elektronisches Zahlungsverkehrsystem nach Anspruch 37, dadurch gekennzeichnet, daß das genannte Transaktionsmodul (4) ebenfalls Online-Transaktionen mit dem genannten Terminalmodul (5) ausführt, und wobei das genannte erste Terminalmodul (5) auch Intermediärfunktionen in Verbindung mit dem genannten Transaktionsmodul (4) ausführt.

39. Elektronisches Zahlungsverkehrsystem nach Anspruch 37, dadurch gekennzeichnet, daß das genannte Geldgeneratormodul (6) und das genannte erste Terminalmodul (5) in einer elektronischen Verarbeitungsvorrichtung vorgesehen sind, die durch den genannten ersten Prozessor gesteuert wird.

40. Elektronisches Zahlungsverkehrsystem nach Anspruch 29, dadurch gekennzeichnet, daß die genannten ersten und zweiten Abrechnungssysteme während Einzahlungen und Auszahlungen der genannten elektronischen Darstellungen von Geld (11) Forderungskonten und Durchführungskonten führen.

41. Elektronisches Zahlungsverkehrsystem nach Anspruch 37, dadurch gekennzeichnet, daß es sich bei dem genannten Geldgenerator, den genannten Transaktions- und Terminalmodulen (6, 4, 5) um eingriffsichere Vorrichtungen handelt, die über kryptographisch sichere Sitzungen kommunikationsfähig sind.

42. Elektronisches Zahlungsverkehrsystem nach Anspruch 41, dadurch gekennzeichnet, daß sich jedes der genannten Module durch Protokollierung einer Transaktion verpflichten kann, so daß kein Abbruch der genannten Transaktion durch Wiederherstellung des Zustands durchgeführt werden kann; und wobei jedes der genannten Module während der genannten Transaktion durch Befolgen einer programmierten Abbruchroutine einen Abbruch durchführen kann, wobei die Steuerung von anderen Routinen oder einem Unterbrechungsprotokoll übertragen wird.

43. Elektronisches Zahlungsverkehrsystem, das folgendes umfaßt:

eine Mehrzahl computergesteuerter Abrechnungssysteme, die einer Mehrzahl von Emissionsbanken (1) zugeordnet sind;
eine Mehrzahl der genannten Mehrzahl von Emissionsbanken zugeordneter Geldgeneratormodule (6), die elektronische Darstellungen von Geld (11) erzeugen, wobei auf Geldemissions-Passivkonten in den genannten Abrechnungssystemen Beträge gutgeschrieben werden, die den erzeugten elektronischen Darstellungen von Geld zugeordnet sind;
eine Mehrzahl der genannten Mehrzahl von Emissionsbanken (1) zugeordneter Terminalmodule (5), die die genannten elektronischen Darstellungen von Geld (11) speichern können;
ein Datenverarbeitungssystem, das einer Clearingbank zugeordnet ist, das die genannten elektronischen Darstellungen von Geld verrechnet und ein Clearingbank-Abrechnungssystem führt, in dem jede der Mehrzahl von Emissionsbanken ein Konto aufweist;
wobei jede der genannten elektronischen Darstellungen von Geld (11) einen Emissionsbankidentifizierer aufweist; und
wobei jedes der Module der genannten Mehrzahl von Terminalmodulen (5) elektronische Darstellungen von Geld (11), die bei dessen Emissionsbank (1) eingezahlt werden, jedoch von einer anderen Emissionsbank (1) ausbezahlt werden, zu der genannten Clearingbank (3) übermittelt, so daß die genannten Emissionsbankenkonten ausgeglichen werden und so daß jede der genannten elektronischen Darstellungen von Geld (11) zurück zu der genannten Emissionsbank (1) übermittelt werden, die durch deren Emissionsbankidentifizierer bezeichnet wird.

44. Elektronisches Zahlungsverkehrsystem nach Anspruch 43, dadurch gekennzeichnet, daß mindestens eines der genannten Geldgeneratormodule (6) und eines der genannten Terminalmodule (5) in einer Vorrichtung mit einem einzigen Prozessor vorgesehen sind.

45. Elektronisches Zahlungsverkehrsystem nach Anspruch 43, dadurch gekennzeichnet, daß die genannten Abrechnungssysteme während der Verrechnung bzw. dem Clearing der genannten elektronischen Darstellungen von

Geld (11) Duchgangskonten und Führungskonten führen.

46. Elektronisches Zahlungsverkehrsystem nach Anspruch 43, dadurch gekennzeichnet, daß es sich bei den genannten Geldgeneratormodulen (6) und den genannten Terminalmodulen (5) um eingriffsichere Vorrichtungen handelt, die über kryptographisch sichere Sitzungen kommunikationsfähig sind.

47. Elektronisches Zahlungsverkehrsystem nach Anspruch 46, dadurch gekennzeichnet, daß sich jedes der genannten Module durch Protokollierung einer Transaktion verpflichten kann, so daß kein Abbruch der genannten Transaktion durch Wiederherstellung des Zustands durchgeführt werden kann; und wobei jedes der genannten Module während der genannten Transaktion durch Befolgen einer programmierten Abbruchroutine einen Abbruch durchführen kann, wobei die Steuerung von anderen Routinen oder einem Unterbrechungsprotokoll übertragen wird.

48. Elektronisches Zahlungsverkehrsystem, das folgendes umfaßt:

eine Mehrzahl computergesteuerter Abrechnungssysteme, die einer Mehrzahl von Emissionsbanken (1) zugeordnet sind;
eine Mehrzahl der genannten Mehrzahl von Emissionsbanken zugeordneter Geldgeneratormodule (6), die elektronische Kreditzusagen (11) erzeugen, wobei Kreditrahmen von Teilnehmer-Darlehenskonten in den genannten Abrechnungssystemen um Beträge in Anspruch genommen werden, die den genannten erzeugten elektronischen Kreditzusagen entsprechen;
eine Mehrzahl der genannten Mehrzahl von Emissionsbanken (1) zugeordneter Terminalmodule (5), die die genannten elektronischen Kreditzusagen (11) speichern können;
ein Datenverarbeitungssystem, das einer Clearingbank zugeordnet ist, das die genannten elektronischen Kreditzusagen verrechnet und ein Clearingbank-Abrechnungssystem führt, in dem jede Emissionsbank der genannten Mehrzahl von Emissionsbanken ein Konto aufweist;
wobei jede der genannten elektronischen Kreditzusagen (11) einen Emissionsbankidentifizierer aufweist; und wobei jedes Terminalmodul (5) der genannten Mehrzahl von Terminalmodulen elektronische Kreditzusagen (11), die auf deren Emissionsbank (1) gutgeschrieben sind, die jedoch von einer anderen Emissionsbank (1) gewährt worden sind, zu einer Clearingbank (3) übermittelt, so daß die Emissionsbankenkonten ausgeglichen werden und so daß jede der genannten elektronischen Kreditzusagen (11) zurück zu der genannten Emissionsbank (1) übermittelt wird, die durch deren Emissionsbankidentifizierer bezeichnet ist.

49. Elektronisches Zahlungsverkehrsystem nach Anspruch 48, dadurch gekennzeichnet, daß mindestens eines der genannten Geldgeneratormodule (6) und eines der genannten Terminalmodule (5) in einer Vorrichtung mit einem einzigen Prozessor vorgesehen sind.

50. Elektronisches Zahlungsverkehrsystem nach Anspruch 48, dadurch gekennzeichnet, daß die genannten Abrechnungssysteme während der Verrechnung bzw. dem Clearing der genannten elektronischen Kreditzusagen (11) Durchgangskonten und Forderungskonten führen.

51. Elektronisches Zahlungsverkehrsystem nach Anspruch 48, dadurch gekennzeichnet, daß es sich bei den genannten Geldgeneratormodulen (6) und den genannten Terminalmodulen (5) um eingriffsichere Vorrichtungen handelt, die über kryptographisch sichere Sitzungen kommunikationsfähig sind.

52. Elektronisches Zahlungsverkehrsystem nach Anspruch 51, dadurch gekennzeichnet, daß sich jedes der genannten Module durch Protokollierung einer Transaktion verpflichten kann, so daß kein Abbruch der genannten Transaktion durch Wiederherstellung des Zustands durchgeführt werden kann; und wobei jedes der genannten Module während der genannten Transaktion durch Befolgen einer programmierten Abbruchroutine einen Abbruch durchführen kann, wobei die Steuerung von anderen Routinen oder einem Unterbrechungsprotokoll übertragen wird.

53. Elektronisches Zahlungsverkehrsystem, das folgendes umfaßt:

ein computergesteuertes Abrechnungssystem sowie ein computerimplementiertes Geldemissions-Abstimmungssystem (23), das einer Emissionsbank (1) zugeordnet ist;
ein der genannten Emissionsbank zugeordnetes Geldgeneratormodul, das elektronische Darstellungen von Geld (11) erzeugt, die in dem genannten Abrechnungssystem abgerechnet werden;
ein der genannten Emissionsbank (1) zugeordnetes Terminalmodul (5), das die genannten Darstellungen von Geld (11) speichern kann;

wobei die genannten Darstellungen von Geld (11) ein Notenverzeichnis aufweisen, das zur eindeutigen Identifizierung jeder der genannten elektronischen Darstellungen von Geld (11) verwendet wird, und mit einer Liste von Übertragungsdatensätzen, die dazu dienen, eine Wertunterteilung jeder der genannten elektronischen Darstellungen von Geld vorzusehen;
wobei das genannte Geldemissions-Abstimmungssystem (23) einen von dem genannten Geldgeneratormodul abgeleiteten Datensatz der genannten elektronischen Darstellungen von Geld (11) führt, die von der genannten Emissionsbank (1) emittiert werden; und
wobei die genannten eingezahlten elektronischen Darstellungen von Geld (11) zu dem genannten Geldemissions-Abstimmungssystem (23) übermittelt werden, das einen Prozessor zur Abstimmung des genannten Datensatzes der emittierten elektronischen Darstellungen von Geld (11) mit den eingezahlten unterteilten elektronischen Darstellungen von Geld (11) aufweist; und
wobei unabgestimmte Fälle Notenfälschungen in dem genannten elektronischen Zahlungsverkehrsystem anzeigen können.

54. Elektronisches Zahlungsverkehrsystem nach Anspruch 53, dadurch gekennzeichnet, daß das genannte Geldgeneratormodul (6) und das genannte Terminalmodul (5) in einer Vorrichtung mit einem einzigen Prozessor vorgesehen sind.

55. Elektronisches Zahlungsverkehrsystem nach Anspruch 53, dadurch gekennzeichnet, daß sich jedes der genannten Module durch Protokollierung einer Transaktion verpflichten kann, so daß kein Abbruch der genannten Transaktion durch Wiederherstellung des Zustands durchgeführt werden kann; und wobei jedes der genannten Module während der genannten Transaktion durch Befolgen einer programmierten Abbruchroutine einen Abbruch durchführen kann, wobei die Steuerung von anderen Routinen oder einem Unterbrechungsprotokoll übertragen wird.

56. Elektronisches Zahlungsverkehrsystem, das folgendes umfaßt:

ein computergesteuertes Abrechnungssystem sowie ein computerimplementiertes Transaktions-Abstimmungssystem (22), das einer Emissionsbank (1) zugeordnet ist;
ein der genannten Emissionsbank zugeordnetes Geldgeneratormodul, das elektronische Darstellungen von Geld erzeugt, die in dem genannten Abrechnungssystem abgerechnet werden;
ein der genannten Emissionsbank (1) zugeordnetes Terminalmodul (5), das die genannten elektronischen Darstellungen von Geld (11) speichern kann;
wobei Transaktionsdatensätze von dem genannten Geldgeneratormodul (6), dem genannten Terminalmodul (5) und dem genannten Online-Abrechnungssystem periodisch zu dem genannten Transaktions-Abstimmungssystem (22) weitergeleitet werden;
wobei das genannte Transaktions-Abstimmungssystem (22) einen Prozessor zum Analysieren der genannten Transaktionsdatensätze aufweist, um sicherzustellen, daß die Terminaltransaktionen mit den entsprechenden Abrechnungstransaktionen übereinstimmen, und um sicherzustellen, daß die Geldgeneratormodultransaktionen mit den entsprechenden Terminaltransaktionen und Abrechnungstransaktionen übereinstimmen; und
wobei etwaige falsche Übereinstimmungen eine unvollkommene Verarbeitung oder einen Sicherheitsverstoß anzeigen können.

57. Elektronisches Zahlungsverkehrsystem nach Anspruch 56, dadurch gekennzeichnet, daß das genannte Geldgeneratormodul (6) und das genannte Terminalmodul (5) in einer Vorrichtung mit einem einzigen Prozessor vorgesehen sind.

58. Elektronisches Zahlungsverkehrsystem nach Anspruch 56, dadurch gekennzeichnet, daß sich jedes der genannten Module durch Protokollierung einer Transaktion verpflichten kann, so daß kein Abbruch der genannten Transaktion durch Wiederherstellung des Zustands durchgeführt werden kann; und wobei jedes der genannten Module während der genannten Transaktion durch Befolgen einer programmierten Abbruchroutine einen Abbruch durchführen kann, wobei die Steuerung von anderen Routinen oder einem Unterbrechungsprotokoll übertragen wird.

Revendications

1. Système monétaire électronique comprenant :

   - un système de comptabilité commandé par ordinateur, associé à une banque émettrice (1),

- un module producteur de monnaie (6), associé à la banque émettrice (1), qui produit des représentations électroniques d'argent (11), dans lequel un compte d'engagement sur la monnaie émise, du système de comptabilité, est crédité d'un montant associé à des représentations électroniques produites d'argent,
- un module caissier (5) associé à la banque émettrice (1), à même de mémoriser lesdites représentations électroniques d'argent (11), et de servir d'intermédiaire pour des transactions bancaires impliquant lesdites représentations électroniques d'argent (11),
- un module de transaction (4) à même de mémoriser lesdites représentations électroniques d'argent (11), d'exécuter des transactions en ligne avec le module caissier (5) et d'échanger lesdites représentations électroniques d'argent (11) avec d'autres modules de transaction (4) dans des transactions en différé,
- lesdites représentations électroniques d'argent (11) comprenant chacune une valeur monétaire de départ produite par le module producteur de monnaie (6), un valeur monétaire transférée et un identificateur de module qui désigne le module qui a reçu ladite représentation électronique d'argent (11), et
- les modules caissier et de transaction (5, 4) comportant des processeurs qui, lorsque lesdits modules (5, 4) sont en cours de fonctionnement en tant que modules cédants transférant une des représentations électroniques d'argent (11) à un module cessionnaire, agissent pour produire un enregistrement de transfert comprenant la valeur monétaire transférée et l'identificateur du module cessionnaire et pour inclure l'enregistrement de transfert et la valeur monétaire de départ dans la représentation électronique d'argent transférée.

2. Système monétaire électronique suivant la revendication 1, caractérisé en ce que le module producteur de monnaie (6) et le module caissier (5) sont réunis dans un dispositif comportant un unique processeur.

3. Système monétaire électronique suivant la revendication 1, caractérisé en ce que le module de transaction (4) et le module caissier (5) ont chacun un répertoire de billets en vue de garder une trace d'une valeur monétaire courante pour chacune des représentations électroniques d'argent (11) qui y sont mémorisées.

4. Système monétaire électronique suivant la revendication 3, caractérisé en ce que la valeur monétaire courante enregistrée dans le répertoire de billets (39) du module cédant, et associée à l'une desdites représentations électroniques d'argent (11) qui y sont mémorisées, est diminuée de ladite valeur monétaire transférée lors d'un transfert, au module cessionnaire, de la représentation électronique d'argent (11) transférée.

5. Système monétaire électronique suivant la revendication 1, caractérisé en ce que les représentations électroniques d'argent (11) susdites comprennent une signature numérique de producteur de monnaie, produite par le producteur de monnaie (6), et une signature numérique de cédant, produite par le module cédant.

6. Système monétaire électronique suivant la revendication 5, caractérisé en ce que les représentations électroniques d'argent (11) susdites comprennent des certificats correspondant à la signature numérique du producteur de monnaie et à la signature numérique du cédant, chacun des certificats comprenant un identificateur de module et une première clé cryptographique du producteur précité de signature numérique, et en ce que la première clé cryptographique est utilisée pour valider ladite signature numérique correspondante.

7. Système monétaire électronique suivant la revendication 6, caractérisé en ce que les certificats sont signés numériquement par un serveur de sécurité (27) associé à une agence de certification (28) et en ce que lesdits certificats peuvent être validés en utilisant une seconde clé cryptographique du serveur de sécurité (27), qui est disponible pour le module caissier (5) et pour le module de transaction (4).

8. Système monétaire électronique suivant la revendication 1, caractérisé en ce que l'enregistrement de transfert comprend en outre une indication de la date du transfert.

9. Système monétaire électronique suivant la revendication 1, caractérisé en ce que les représentations électroniques d'argent (11) susdites comprennent une liste d'enregistrements de transfert qui comportent chacun un identificateur du module cessionnaire.

10. Système monétaire électronique suivant la revendication 9, caractérisé en ce que le module cessionnaire vérifie que le dernier enregistrement de transfert, dans la représentation électronique d'argent (11) transférée susdite, comporte un identificateur de module cessionnaire qui est le même qu'un identificateur de module du module cédant.

11. Système monétaire électronique suivant la revendication 1, caractérisé en ce que les modules producteur de

monnaie, caissier, et de transaction (6. 5. 4) sont des dispositifs à l'abri d'une falsification et qui sont à même de communiquer par l'intermédiaire de cessions cryptographiquement sûres.

12. Système monétaire électronique suivant la revendication 11, caractérisé en ce que chacun des modules (6, 5, 4) précités est configuré pour exécuter une tâche à la manière d'un co-processeur modulaire d'un dispositif de traitement électronique.

13. Système monétaire électronique suivant la revendication 11, caractérisé en ce que chaque module (6, 5, 4) précité peut s'engager en inscrivant une transaction de façon à ce qu'il ne puisse plus abandonner l'exécution de ladite transaction en faisant reculer son état, et en ce que chaque module peut abandonner l'exécution pendant ladite transaction en suivant un sous-programme d'abandon programmé dans lequel la commande est transférée d'autres sous-programmes ou d'un protocole à délai d'attente au sous-programme d'abandon.

14. Système monétaire électronique comprenant :

- un système de comptabilité commandé par ordinateur, associé à une banque émettrice (1),
- un module producteur de monnaie (6), associé à la banque émettrice (1), qui produit des représentations électroniques d'argent (11), dans lequel un compte d'engagement sur la monnaie émise, du système de comptabilité, est crédité d'un montant associé à des représentations électroniques produites d'argent,
- un module caissier (5) associé à la banque émettrice (1), à même de mémoriser lesdites représentations électroniques d'argent (11), et de servir d'intermédiaire pour des transactions bancaires impliquant lesdites représentations électroniques d'argent (11),
- un module de transaction (4) à même de mémoriser lesdites représentations électroniques d'argent (11), d'exécuter des transactions en ligne avec le module caissier (5) et d'échanger lesdites représentations électroniques d'argent (11) avec d'autres modules de transaction (4) dans des transactions en différé,
- lesdites représentations électroniques d'argent (11) comprenant une date d'expiration,
- les autres modules de transaction (4) comportant des processeurs adaptés pour refuser d'accepter des transferts entrepris desdites représentations électroniques d'argent (11) lorsque les transferts entrepris ont lieu après la date d'expiration desdites représentations électroniques d'argent (11).

15. Système monétaire électronique suivant la revendication 14, caractérisé en ce que le module producteur de monnaie (6) et le module caissier (5) sont réunis dans un dispositif comportant un unique processeur.

16. Système monétaire électronique suivant la revendication 14, caractérisé en ce que le système de comptabilité précité entretient des comptes de monnaie due et de monnaie en transit, pendant des dépôts et retraits desdites représentations électroniques d'argent (11).

17. Système monétaire électronique suivant la revendication 14, caractérisé en ce que la date d'expiration varie en fonction d'une valeur monétaire associée aux représentations électroniques d'argent (11) précitées.

18. Système monétaire électronique suivant la revendication 14, caractérisé en ce que les représentations électroniques d'argent (11) mémorisées dans le module de transaction (4) sont mises à jour lorsqu'il est en transaction avec le module caissier (5).

19. Système monétaire électronique suivant la revendication 18, caractérisé en ce que les représentations électroniques d'argent (11) précitées sont mises à jour par le module de transaction (4) en cours de transfert desdites représentations électroniques d'argent (11) mémorisées vers le module caissier (5), le module producteur de monnaie (6) produisant une nouvelle représentation électronique d'argent (11) de remplacement, comportant une nouvelle date d'expiration, le module caissier (5) transférant la nouvelle représentation électronique d'argent (11) de remplacement vers le module de transaction (4) précité.

20. Système monétaire électronique suivant la revendication 14, caractérisé en ce que les modules producteur de monnaie, caissier, et de transaction (4) sont des dispositifs à l'abri d'une falsification et qui sont à même de communiquer par l'intermédiaire de cessions cryptographiquement sûres.

21. Système monétaire électronique suivant la revendication 20, caractérisé en ce que chaque module précité peut s'engager en inscrivant une transaction de façon à ce qu'il ne puisse plus abandonner l'exécution de ladite transaction en faisant reculer son état, et en ce que chaque module peut abandonner l'exécution pendant ladite tran-

saction en suivant un sous-programme d'abandon programmé dans lequel la commande est transférée d'autres sous-programmes ou d'un protocole à délai d'attente au sous-programme d'abandon.

22. Système monétaire électronique comprenant :

- un système de comptabilité commandé par ordinateur, associé à une banque émettrice (1),
- un module producteur de monnaie (6), associé à la banque émettrice (1), qui produit des représentations électroniques d'argent (11), dans lequel un compte d'engagement sur la monnaie émise, du système de comptabilité, est crédité d'un montant associé à des représentations électroniques produites d'argent,
- un module caissier (5) associé à la banque émettrice (1), à même de mémoriser lesdites représentations électroniques d'argent (11), et de servir d'intermédiaire pour des transactions bancaires impliquant lesdites représentations électroniques d'argent (11),
- un module de transaction (4) à même de mémoriser lesdites représentations électroniques d'argent (11), d'exécuter des transactions en ligne avec le module caissier (5) et d'échanger lesdites représentations électroniques d'argent (11) avec d'autres modules de transaction (4) dans des transactions en différé,
- un serveur de sécurité (27) utilisé pour mettre en oeuvre la sécurité du système monétaire électronique,
- le module producteur de monnaie (6), le module caissier (5) et le module de transaction (4) étant associés chacun à un identificateur de module unique contenu dans un certificat qui est signé numériquement par le serveur de sécurité (27), les certificats n'étant valables que pendant une période de temps limitée, le module associé n'étant pas à même de faire des transactions avec d'autres modules après ce temps, jusqu'à ce qu'un nouveau certificat soit obtenu,
- le nouveau certificat et des identificateurs de modules compromis étant obtenus lorsque le module effectue une première connexion de réseau à un réseau comportant un ou plusieurs serveurs de sécurité,
- le module ne faisant pas de transaction avec un quelconque autre module comportant un des identificateurs de modules compromis.

23. Système monétaire électronique suivant la revendication 22, caractérisé en ce que le module producteur de monnaie (6) et le module caissier (5) sont réunis dans un dispositif comportant un unique processeur.

24. Système monétaire électronique suivant la revendication 22, caractérisé en ce que le système de comptabilité précité entretient des comptes de monnaie due et de monnaie en transit, pendant des dépôts et retraits desdites représentations électroniques d'argent (11).

25. Système monétaire électronique suivant la revendication 22, caractérisé en ce que le serveur de sécurité (27) distribue, sur demande, une clé de certification.

26. Système monétaire électronique suivant la revendication 22, caractérisé en ce que le serveur de sécurité (27) signe de façon numérique un profil de compte qui comporte des zones de données comprenant un identificateur de banque, un numéro de compte et une indication d'un type de compte, le profil de compte étant utilisé par le module de transaction (4) pour accéder à un compte de titulaire identifié par le numéro ce compte.

27. Système monétaire électronique suivant la revendication 22, caractérisé en ce que le module producteur de monnaie (6), le module caissier (5), le module de transaction (4) et le serveur de sécurité (27) sont des dispositifs à l'abri d'une falsification, à même de communiquer par l'intermédiaire de cessions cryptographiquement sûres.

28. Système monétaire électronique suivant la revendication 27, caractérisé en ce que chaque module précité et le serveur de sécurité (27) peuvent s'engager en inscrivant une transaction de façon à ce qu'ils ne puissent plus abandonner l'exécution de la transaction en faisant reculer son état, et en ce que chaque module et le serveur de sécurité (27) peuvent abandonner l'exécution pendant ladite transaction en suivant un sous-programme d'abandon programmé dans lequel la commande est transférée d'autres sous-programmes ou d'un protocole à délai d'attente au sous-programme d'abandon précité.

29. Système monétaire électronique comprenant :

- un système de comptabilité commandé par ordinateur, associé à une banque émettrice (1),
- un module producteur de monnaie (6), associé à la banque émettrice, qui produit des autorisations (11) de crédit électroniques, dans lequel une ligne de crédit d'un compte de crédit d'un titulaire, du système de comptabilité, est accru d'un montant associé à des autorisations de crédit électroniques produites,

- un module caissier (5) associé à la banque émettrice (1), à même de mémoriser ladite autorisation de crédit électronique (11), et de servir d'intermédiaire pour des transactions bancaires impliquant l'autorisation de crédit électronique (11) précitée,
- un module de transaction (4) à même de mémoriser ladite autorisation de crédit électronique (11), d'exécuter des transactions en lignes avec le module caissier (5) et de transférer l'autorisation de crédit électronique (11) vers un autre module de transaction (4) dans une transaction en différé, et
- ladite autorisation de crédit électronique (11) comprenant un numéro de compte du compte de crédit du titulaire, un montant monétaire de départ et une signature numérique produite par le module producteur de monnaie (6),
- l'autorisation de crédit électronique pouvant être transférée entre des modules de transaction pour un montant monétaire transféré inférieur ou égal au montant monétaire de départ, et
- ladite banque émettrice (1) débitant du montant monétaire transféré le compte de crédit du titulaire lorsque l'autorisation de crédit électronique (11) est déposée.

30. Système monétaire électronique suivant la revendication 29, caractérisé en ce que le module producteur de monnaie (6) et le module caissier (5) sont réunis dans un dispositif comportant un unique processeur.

31. Système monétaire électronique suivant la revendication 29, caractérisé en ce que le système de comptabilité entretient des comptes de monnaie due et de monnaie en transit, pendant des dépôts et retraits de ladite autorisation de crédit électronique (11).

32. Système monétaire électronique suivant la revendication 29, caractérisé en ce que le module de transaction (4) ne peut transférer qu'une fois l'autorisation de crédit électronique (11) à un autre module de transaction (4).

33. Système monétaire électronique suivant la revendication 29, caractérisé en ce que les modules producteur de monnaie, caissier, et de transaction (4) sont des dispositifs à l'abri d'une falsification et qui sont à même de communiquer par l'intermédiaire de cessions cryptographiquement sûres.

34. Système monétaire électronique suivant la revendication 33, caractérisé en ce que l'autorisation de crédit électronique (11) comprend des signatures numériques produites par les modules caissier et de transaction (5, 4) lors d'un transfert de ladite autorisation de crédit électronique (11), et en ce que le module producteur de monnaie (6), le module caissier (5) et le module de transaction (4) sont associés chacun à un certificat électronique par lequel d'autres modules peuvent vérifier leur authenticité, le transfert de l'autorisation de crédit électronique (11) par le module de transaction (4) vers l'autre module de transaction (4) précité pouvant être exécuté sans une identification du titulaire.

35. Système monétaire électronique suivant la revendication 33, caractérisé en ce que chaque module précité peut s'engager en inscrivant une transaction de façon à ce qu'il ne puisse plus abandonner l'exécution de ladite transaction en faisant reculer son état, et en ce que chaque module peut abandonner l'exécution pendant ladite transaction en suivant un sous-programme d'abandon programmé dans lequel la commande est transférée d'autres sous-programmes ou d'un protocole à délai d'attente au sous-programme d'abandon.

36. Système monétaire électronique suivant la revendication 29, caractérisé en ce que le module de transaction (4) est à même de mémoriser tant des représentations électroniques d'argent (11) que des autorisations de crédit électroniques (11), et en ce que le module de transaction (4) peut transférer tant des représentations électroniques d'argent (11) que des autorisations de crédit électroniques (11) dans un transfert de transaction unique vers l'autre module de transaction (4) précité par l'intermédiaire de cessions cryptographiquement sûres.

37. Système monétaire électronique comprenant

- un premier système de comptabilité commandé par ordinateur, associé à une banque émettrice (1),
- un module producteur de monnaie, associé à la banque émettrice (1), qui produit des représentations électroniques d'argent, dans lequel un compte d'engagement sur la monnaie émise, du premier système de comptabilité, est crédité d'un montant associé à des représentations électroniques d'argent produites,
- un premier module caissier (5), associé à la banque émettrice (1), à même de mémoriser lesdites représentations électroniques d'argent (11),
- une pluralité de seconds systèmes de comptabilité commandés par ordinateur, chacun étant associé à une banque correspondante (2), chaque banque correspondante conservant un compte dans ledit premier systè-

me de comptabilité,

- une pluralité de seconds modules caissiers (5), chacun étant associé à une des banques correspondantes (2), chacun étant à même de mémoriser lesdites représentations électroniques d'argent (11),
- un module de transaction (4) qui mémorise lesdites représentations électroniques d'argent (11), qui exécute des transactions en ligne avec la pluralité de seconds modules caissiers (5) et qui échange lesdites représentations électroniques d'argent (11) avec d'autres modules de transaction (4) dans des transactions en différé,
- le premier module caissier (5) comportant un premier processeur qui sert d'intermédiaire pour des transactions entre le premier système de comptabilité, le module producteur de monnaie (6) et le second module caissier (5), et
- le second module caissier (5) comportant un second processeur qui sert d'intermédiaire pour des transactions entre le second système de comptabilité, le premier module caissier (5) et le module de transaction (4).

38. Système monétaire électronique suivant la revendication 37, caractérisé en ce que le module de transaction (4) exécute également des transactions en ligne avec le module caissier (5) et en ce que le premier module caissier (5) sert également d'intermédiaire pour des transactions impliquant le module de transaction (4).

39. Système monétaire électronique suivant la revendication 37, caractérisé en ce que le module producteur de monnaie (6) et le premier module caissier (5) sont réunis dans un dispositif de traitement électronique commandé par le premier processeur.

40. Système monétaire électronique suivant la revendication 37, caractérisé en ce que les premier et second systèmes de comptabilité entretiennent des comptes de monnaie due et de monnaie en transit, pendant des dépôts et retraits desdites représentations électroniques d'argent (11).

41. Système monétaire électronique suivant la revendication 37, caractérisé en ce que les modules producteur de monnaie, de transaction et caissiers (6, 4. 5) sont des dispositifs à l'abri d'une falsification, à même de communiquer par l'intermédiaire de cessions cryptographiquement sûres.

42. Système monétaire électronique suivant la revendication 41, caractérisé en ce que chaque module susdit peut s'engager en inscrivant une transaction de façon à ce qu'il ne puisse plus suspendre l'exécution de ladite transaction en faisant reculer son état, et en ce que chaque module peut abandonner l'exécution pendant ladite transaction en suivant un sous-programme d'abandon programmé dans lequel la commande est transférée d'autres sous-programmes ou d'un protocole à délai d'attente au sous-programme d'abandon.

43. Système monétaire électronique comprenant

- une pluralité de systèmes de comptabilité commandés par ordinateur, associés à une pluralité de banques émettrices (1),
- une pluralité de modules producteurs de monnaie (6), associés à la pluralité de banques émettrices (1), qui produisent des représentations électroniques d'argent (11), des comptes d'engagement sur la monnaie émise, desdits systèmes de comptabilité, étant crédités de montants associés à des représentations électroniques produites d'argent,
- une pluralité de modules caissiers (5), associés à la pluralité de banques émettrices (1), à même de mémoriser les représentations électroniques d'argent (11) susdites,
- un système de traitement de données associé à une banque de compensation qui compense les représentations électroniques d'argent et qui entretient un système de comptabilité de banque de compensation dans lequel ladite pluralité de banques émettrices ont chacune un compte,
- chacune des représentations électroniques d'argent (11) comprenant un identificateur de banque émettrice, et
- chacun de la pluralité des modules caissiers (5) envoyant des représentations électroniques d'argent (11), déposées à sa banque émettrice (1) mais émises par une autre banque émettrice (1), à la banque de compensation (3) pour compenser les comptes de banques émettrices précités et pour envoyer chaque représentation électronique d'argent (11) en retour à la banque émettrice (1) indiquée par son identificateur de banque émettrice.

44. Système monétaire électronique suivant la revendication 43, caractérisé en ce qu'au moins un des modules producteurs de monnaie (6) et un des modules caissiers (5) sont réunis dans un dispositif comportant un unique processeur.

45. Système monétaire électronique suivant la revendication 43, caractérisé en ce que les systèmes de comptabilité entretiennent des comptes de monnaie en transit et de monnaie due, pendant une compensation desdites représentations électroniques d'argent (11).

46. Système monétaire électronique suivant la revendication 43, caractérisé en ce que les modules producteurs de monnaie (6) et les modules caissiers (5) sont des dispositifs à l'abri de falsifications, à même de communiquer par l'intermédiaire de cessions cryptographiquement sûres.

47. Système monétaire électronique suivant la revendication 46, caractérisé en ce que chaque module susdit peut s'engager en inscrivant une transaction de façon à ce qu'il ne puisse plus abandonner l'exécution de ladite transaction en faisant reculer son état, et en ce que chaque module peut abandonner l'exécution pendant ladite transaction en suivant un sous-programme d'abandon programmé dans lequel la commande est transférée d'autres sous-programmes ou d'un protocole à délai d'attente au sous-programme d'abandon.

48. Système monétaire électronique comprenant

- une pluralité de systèmes de comptabilité commandés par ordinateur, associés à une pluralité de banques émettrices (1),
- une pluralité de modules producteurs de monnaie (6), associés à la pluralité de banques émettrices, qui produisent des autorisations de crédit électroniques (11), des lignes de crédit de comptes de crédit de titulaire, desdits systèmes de comptabilité, étant accrus par des montants associés à des autorisations de crédit électroniques produites,
- une pluralité de modules caissiers (5) associés à ladite pluralité de banques émettrices (1), à même de mémoriser les autorisations de crédit électroniques (11),
- un système de traitement de données, associé à une banque de compensation, qui compense les autorisations de crédit électroniques et qui entretient un système de comptabilité de banque de compensation dans lequel la pluralité de banques émettrices ont chacune un compte,
- chacune des autorisations de crédit électroniques (11) comportant un identificateur de banque émettrice, et
- chacun de la pluralité des modules caissiers (5) envoyant des autorisations de crédit électroniques (11), déposées à sa banque émettrice (1) mais émises par une autre banque émettrice (1), à la banque de compensation (3) pour compenser les comptes de banques émettrices et pour envoyer chaque autorisation de crédit électronique (11) précitée en retour à la banque émettrice (1) indiquée par son identificateur de banque émettrice.

49. Système monétaire électronique suivant la revendication 48, caractérisé en ce qu'au moins un des modules producteurs de monnaie (6) et un des modules caissiers (5) sont réunis dans un dispositif comportant un unique processeur.

50. Système monétaire électronique suivant la revendication 48, caractérisé en ce que les systèmes de comptabilité précités entretiennent des comptes de monnaie en transit et de monnaie due, pendant une compensation des autorisations de crédit électroniques (11) précitées.

51. Système monétaire électronique suivant la revendication 48, caractérisé en ce que les modules producteursde monnaie (6) et les modules caissiers (5) sont des dispositifs à l'abri d'une falsification, à même de communiquer par des cessions cryptographiquement sûres.

52. Système monétaire électronique suivant la revendication 51, caractérisé en ce que chaque module précité peut s'engager en inscrivant une transaction de façon à ce qu'il ne puisse plus abandonner l'exécution de ladite transaction en faisant reculer son état, et en ce que chaque module peut abandonner l'exécution pendant ladite transaction en suivant un sous-programme d'abandon programmé dans lequel la commande est transférée d'autres sous-programmes ou d'un protocole à délai d'attente au sous-programme d'abandon.

53. Système monétaire électronique comprenant

- un système de comptabilité commandé par ordinateur et, associé à une banques émettrice (1), un système de réconciliation (23) de monnaie émise, mis en oeuvre par ordinateur,
- un module producteur de monnaie, associé à la banque émettrice, qui produit des représentations électroniques de monnale (11) qui sont justifiées dans un système de comptabilité,

- un module caissier (5) associé à la banque émettrice (1), à même de mémoriser les représentations électroniques de monnaie (11),
- les représentations électroniques de monnaie (11) comprenant un identificateur de billet utilisé pour identifier de façon unique chaque représentation électronique de monnaie (11), et une liste d'enregistrements de transferts pour fournir une possibilité de subdiviser des valeurs de chaque représentation électronique de monnaie,
- le système de réconciliation (23) de monnaie émise conservant un enregistrement, dérivé du module producteur de monnaie, des représentations électroniques de monnaie (11) qui ont été émises par la banque émettrice (1), et
- des représentations électroniques de monnaie (11), qui sont déposées, étant envoyées au système de réconciliation (23) de monnaies émises qui a un processeur pour mettre en correspondance l'enregistrement de représentations électroniques de monnaie (11) qui ont été émises et ces représentations électroniques subdivisées de monnaie (11) déposées et
- des cas qui ne correspondent pas pouvant indiquer une contrefaçon de billet dans le système monétaire électronique.

54. Système monétaire électronique suivant la revendication 53, caractérisé en ce que le module producteur de monnaie (6) et le module caissier (5) sont réunis dans un dispositif comportant un processeur unique.

55. Système monétaire électronique suivant la revendication 53, caractérisé en ce que chaque module précité peut s'engager en inscrivant une transaction de façon à ce qu'il ne puisse plus abandonner l'exécution de ladite transaction en faisant reculer son état, et en ce que chaque module peut abandonner l'exécution pendant ladite transaction en suivant un sous-programme d'abandon programmé dans lequel la commande est transférée d'autres sous-programmes ou d'un protocole à délai d'attente au sous-programme d'abandon.

56. Système monétaire électronique comprenant

- un système de comptabilité commandé par ordinateur et, associé à une banque émettrice (1), un système de réconciliation (22) de transaction, mis en oeuvre par ordinateur,
- un module producteur de monnaie, associé à la banque émettrice, qui produit des représentations électroniques de monnaie qui sont justifiées dans le système de comptabilité,
- un module caissier (5) associé à la banque émettrice (1), à même de mémoriser les représentations électroniques de monnaie (11),
- des enregistrements de transaction en provenance du module producteur de monnaie (6), du module caissier (5) et du système de comptabilité en ligne étant périodiquement passés au système de réconciliation de transaction (22),
- le système de réconciliation de transaction (22) comportant un processeur pour analyser les enregistrements de transactions afin de s'assurer que des transactions du caissier correspondent aux transactions de comptabilité appropriées et de s'assurer que des transactions du module producteur de monnaie correspondent aux transactions de caissier et aux transactions de comptabilité appropriées, et
- toute absence de correspondance pouvant indiquer un traitement incomplet ou une violation de la sécurité.

57. Système monétaire électronique suivant la revendication 56, caractérisé en ce que le module producteur de monnaie (6) et le module caissier (5) sont réunis dans un dispositif comportant un processeur unique.

58. Système monétaire électronique suivant la revendication 56, caractérisé en ce que chaque module précité peut s'engager en inscrivant une transaction de façon à ce qu'il ne puisse plus abandonner l'exécution de ladite transaction en faisant reculer son état, et en ce que chaque module peut abandonner l'exécution pendant ladite transaction en suivant un sous-programme d'abandon programmé dans lequel la commande est transférée d'autres sous-programmes ou d'un protocole à délai d'attente au sous-programme d'abandon.

FIG. 1

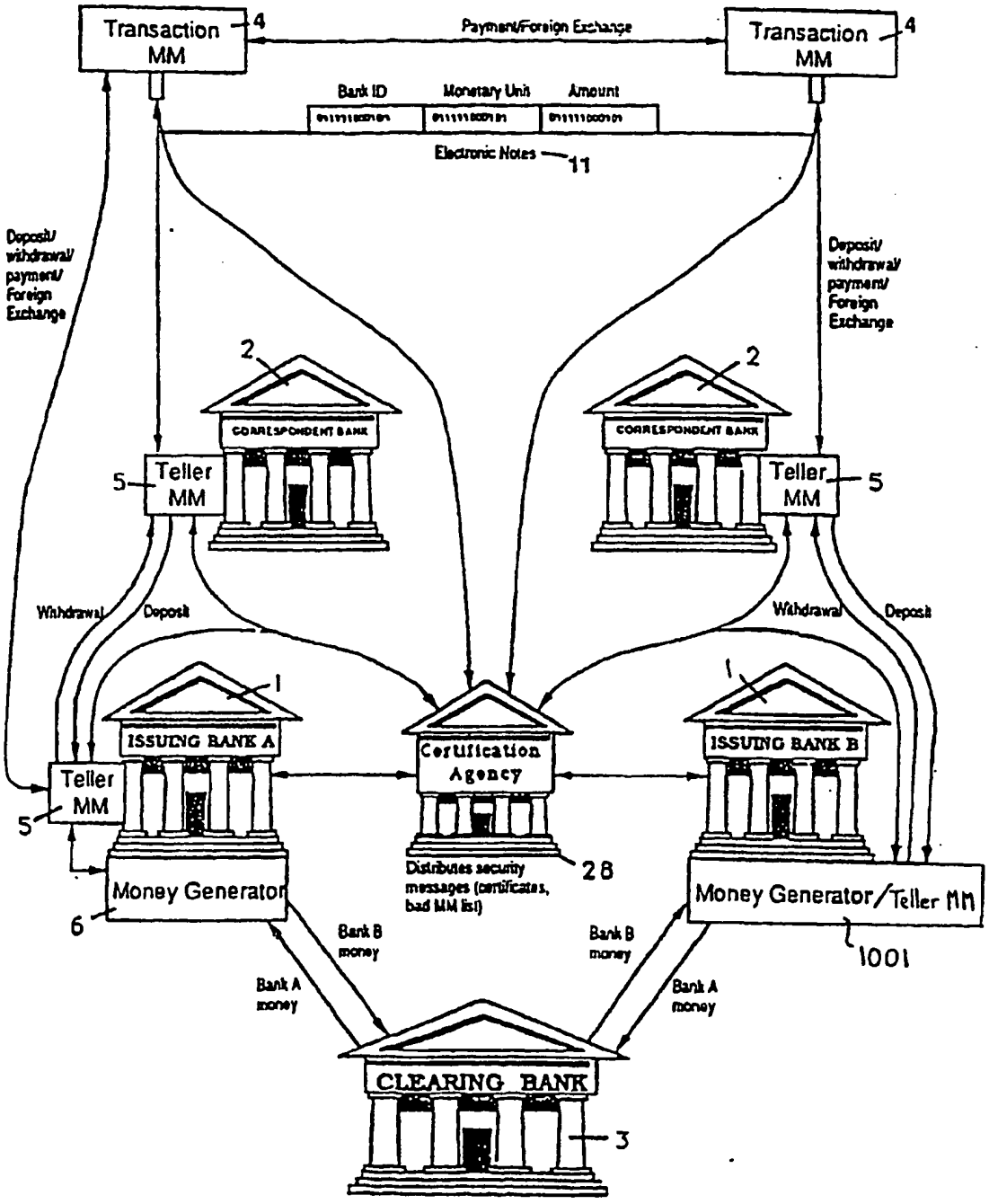
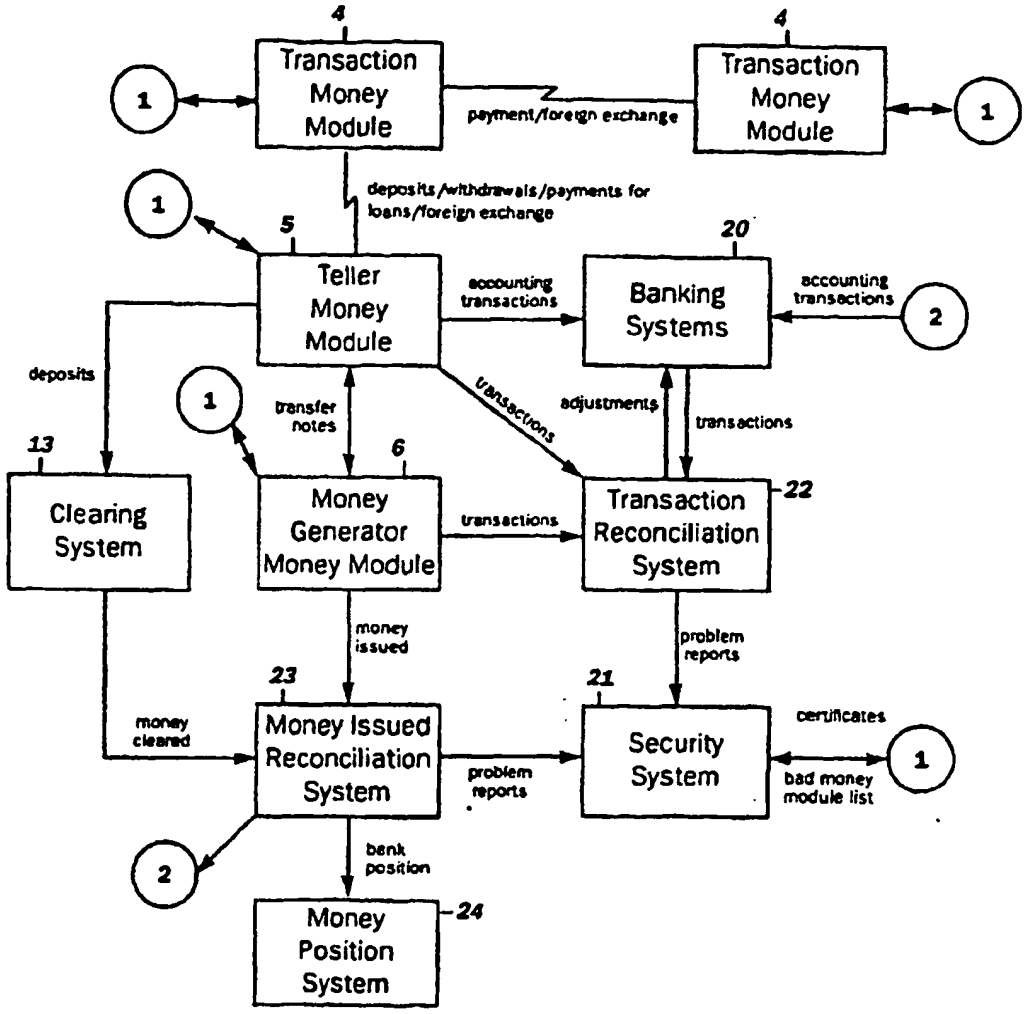

Transaction MM
4
Payment/Foreign Exchange
Transaction MM
4
Bank ID
Monetary Unit
Amount
Electronic Notes
11
Deposit/ withdrawal/ payment/ Foreign Exchange
Deposit/ withdrawal/ payment/ Foreign Exchange
2
CORRESPONDENT BANK
2
CORRESPONDENT BANK
Teller MM
5
Teller MM
5
Withdrawal
Deposit
Withdrawal
Deposit
1
ISSUING BANK A
Certification Agency
1
ISSUING BANK B
Teller MM
5
Money Generator
6
Distributes security messages (certificates, bad MM list)
28
Money Generator/Teller MM
1001
Bank B money
Bank B money
Bank A money
Bank A money
CLEARING BANK
3

FIG. 2



Network **25** (not shown)

Electronic Monetary System

FIG. 3

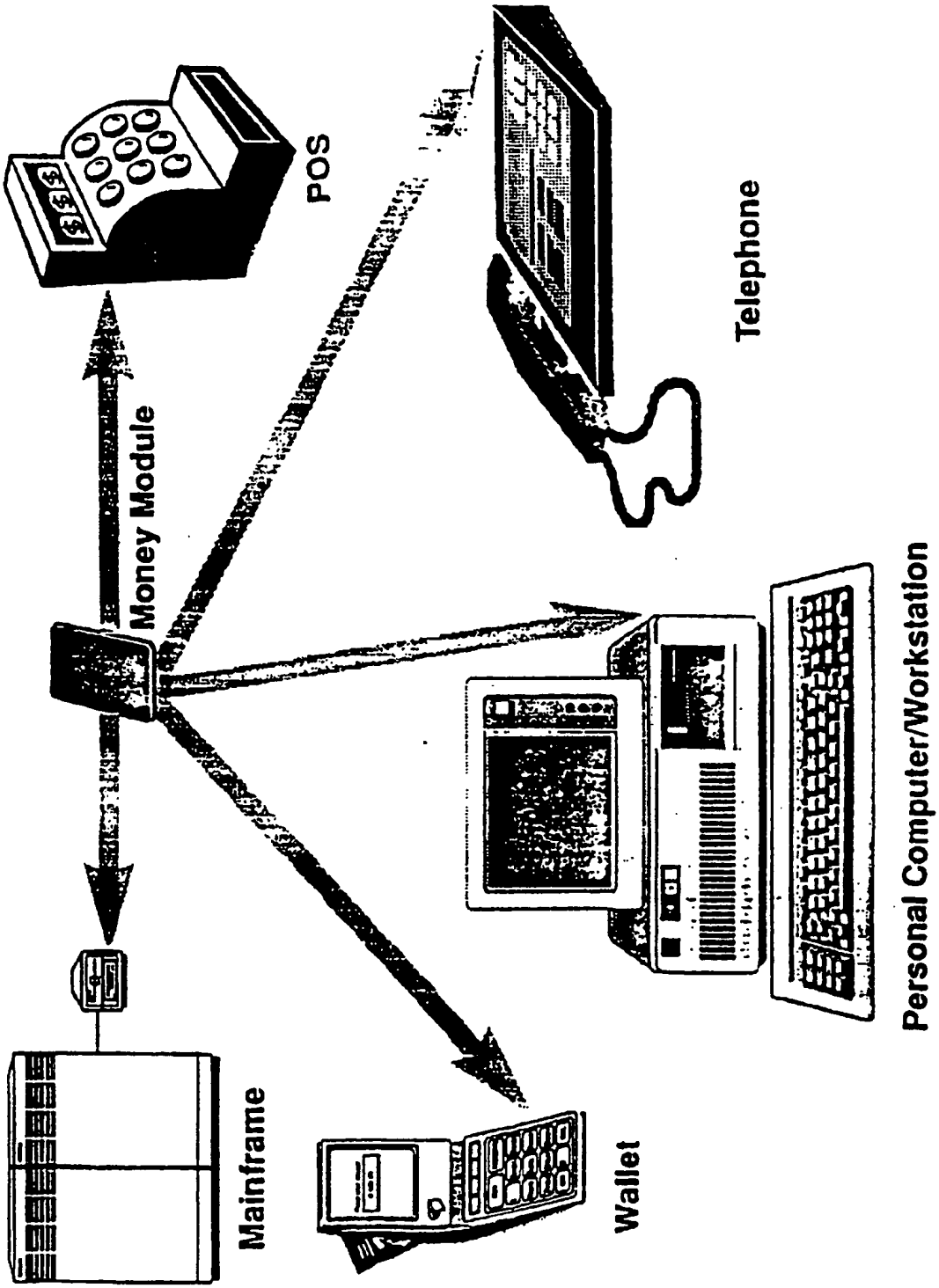
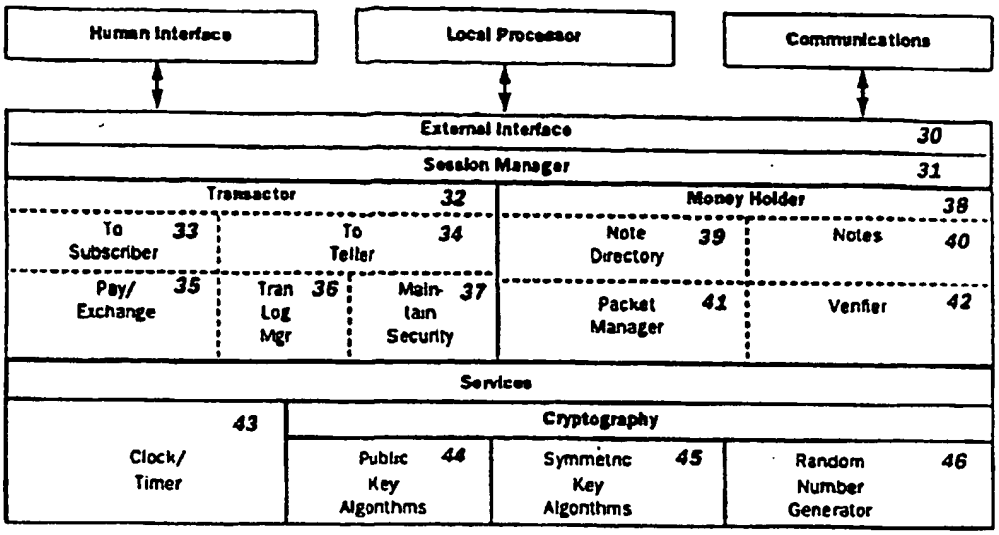
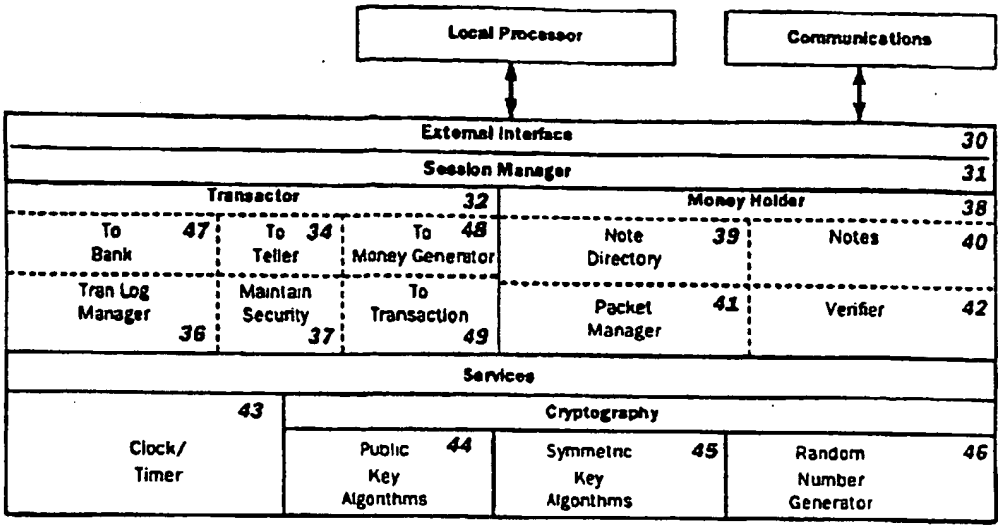

POS
Telephone
Money Module
Personal Computer/Workstation
Mainframe
Wallet

FIG. 4



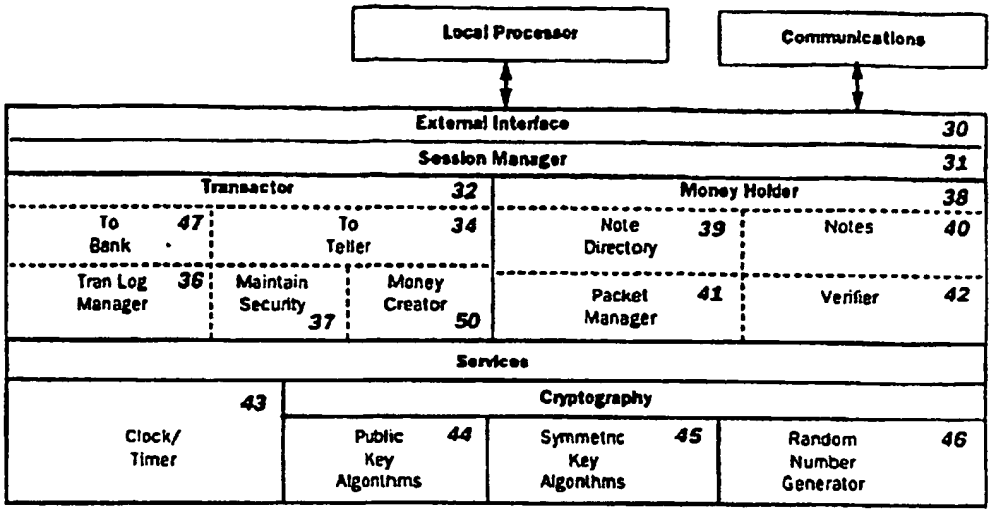
Transaction Money Module

FIG. 5



Teller Money Module

FIG. 6



Money Generator Module

Fig. 7

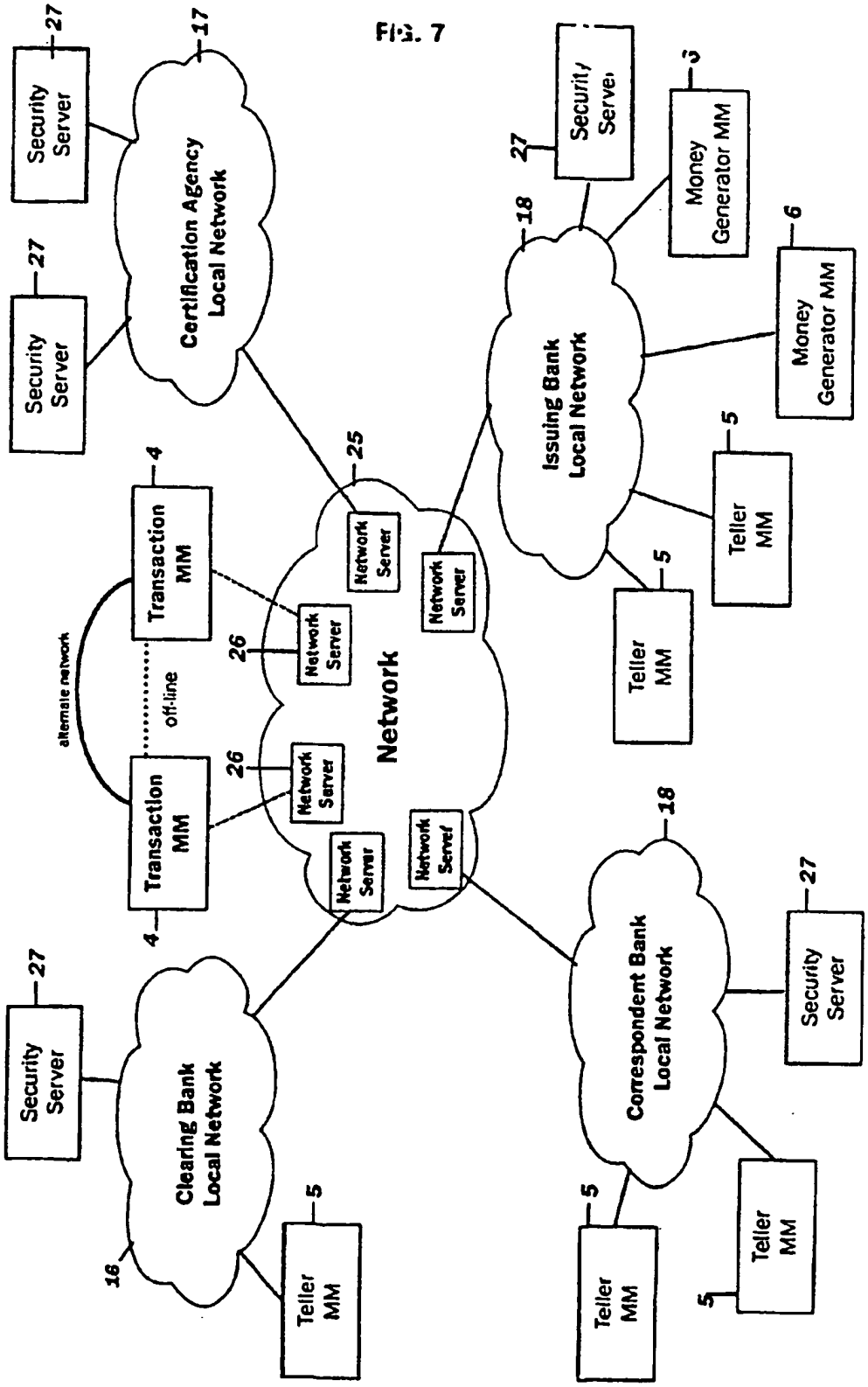

Security Server
27
Certification Agency Local Network
17
Security Server
27
Transaction MM
4
alternate network
off-line
Transaction MM
4
Network Server
26
Network Server
26
Network Server
Network Server
Network Server
Network Server
25
Network
Issuing Bank Local Network
18
Security Server
27
Money Generator MM
3
Money Generator MM
6
Teller MM
5
Teller MM
5
Clearing Bank Local Network
16
Security Server
27
Teller MM
5
Correspondent Bank Local Network
18
Security Server
27
Teller MM
5
Teller MM
5

FIG. 8

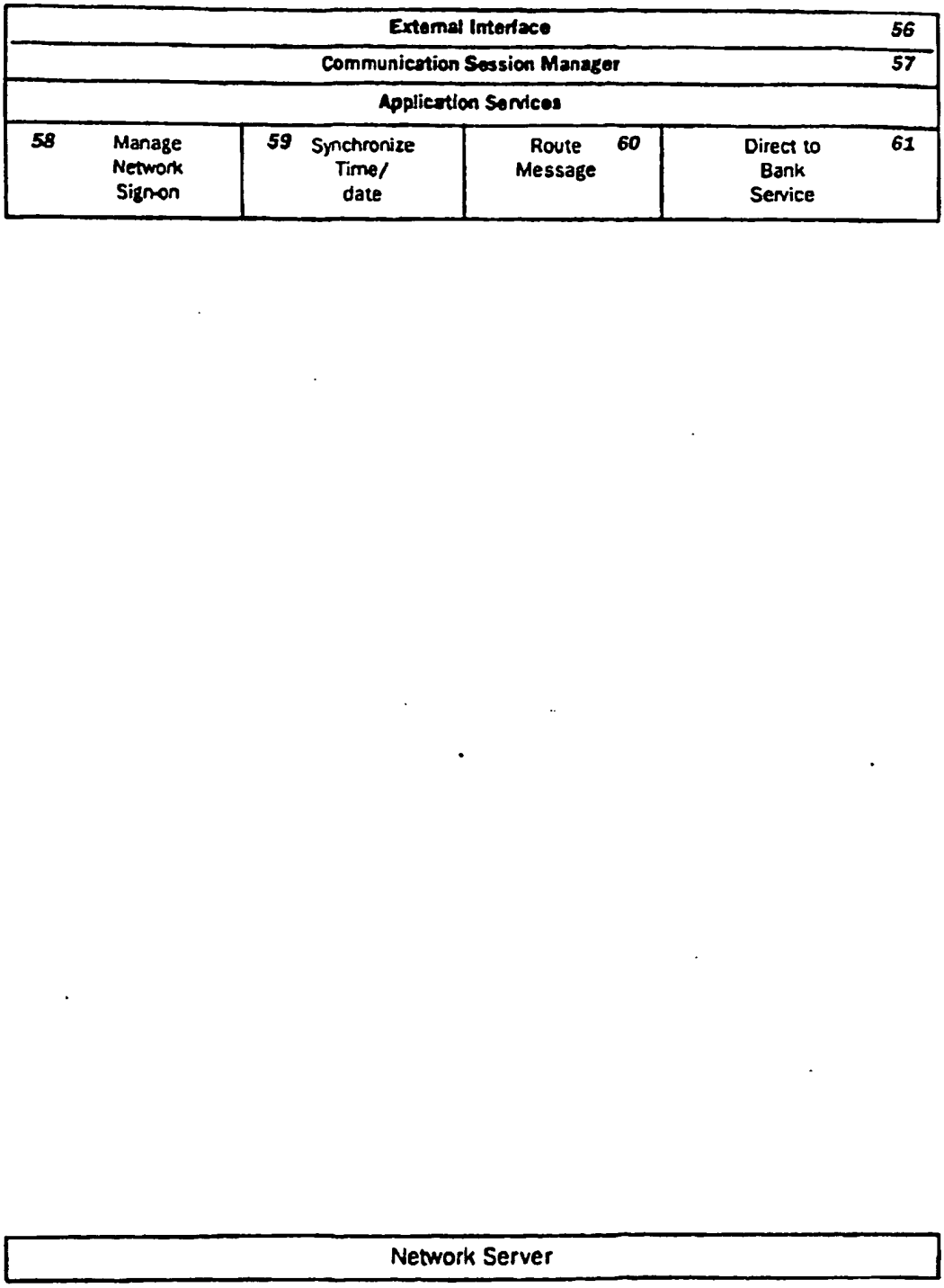
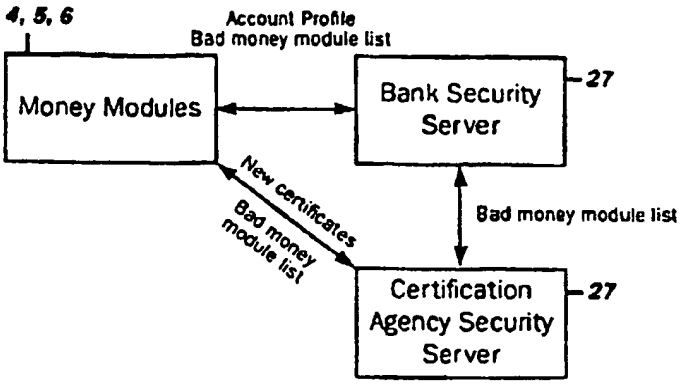
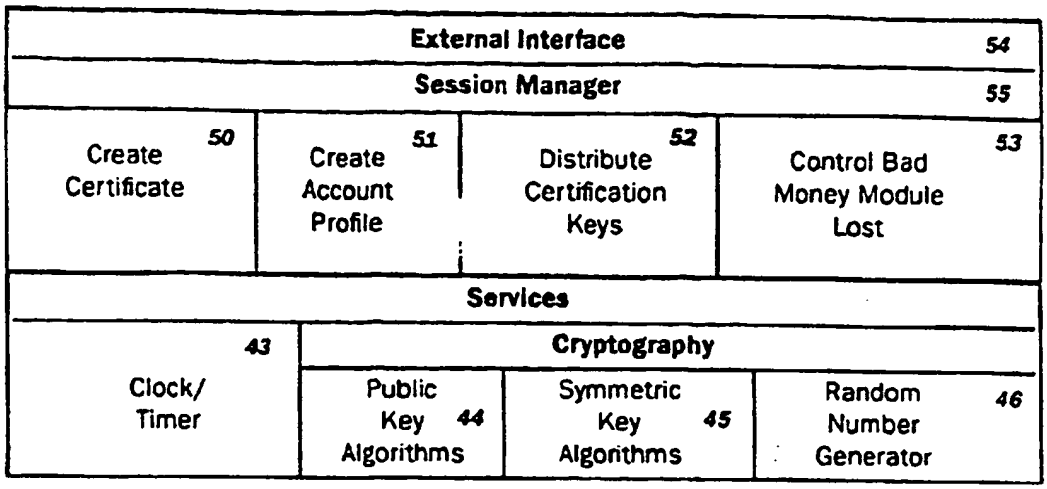

External Interface
56
Communication Session Manager
57
Application Services
58
Manage Network Sign-on
59
Synchronize Time/ date
Route Message
60
Direct to Bank Service
61
Network Server

FIG. 9



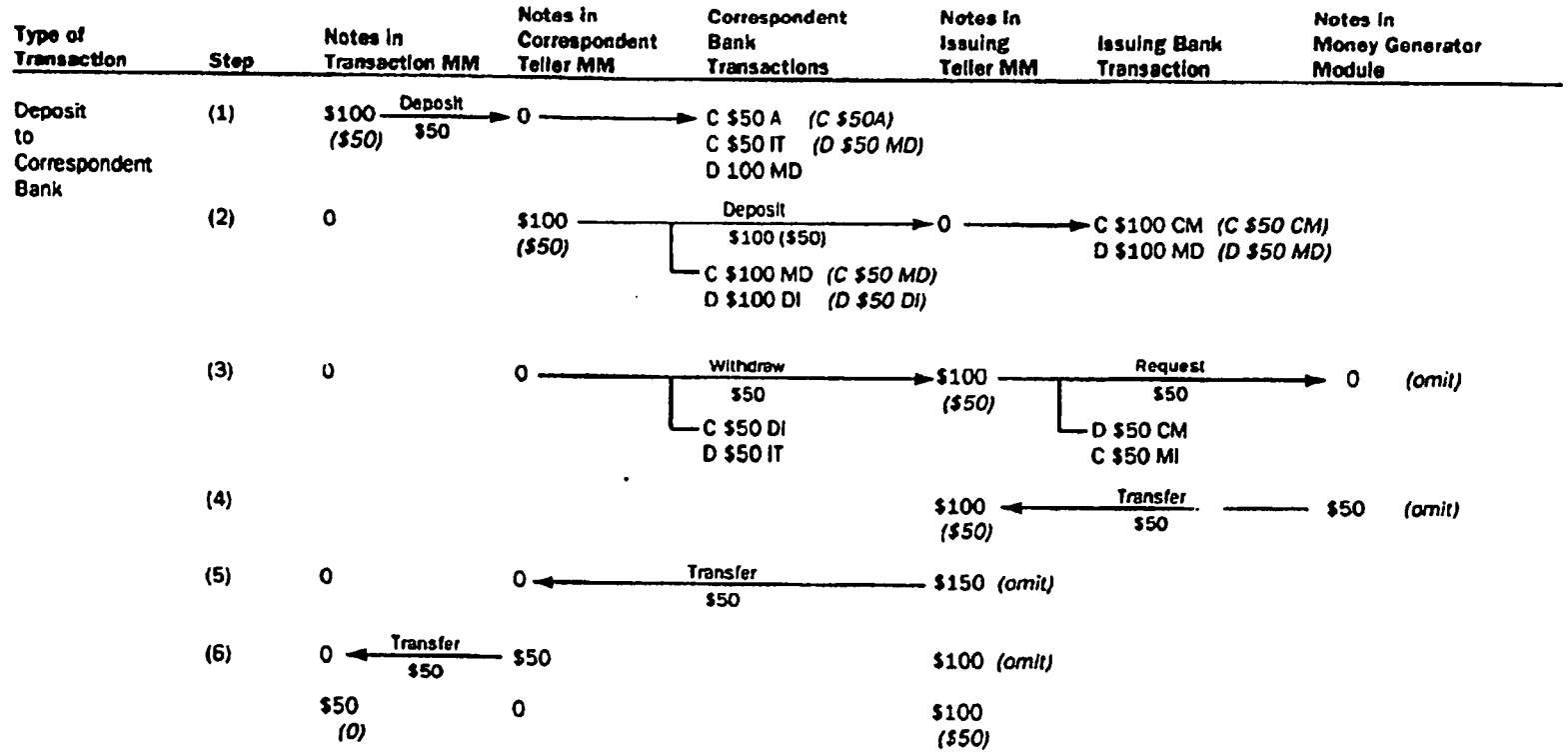
Security System

FIG. 10



Security Server

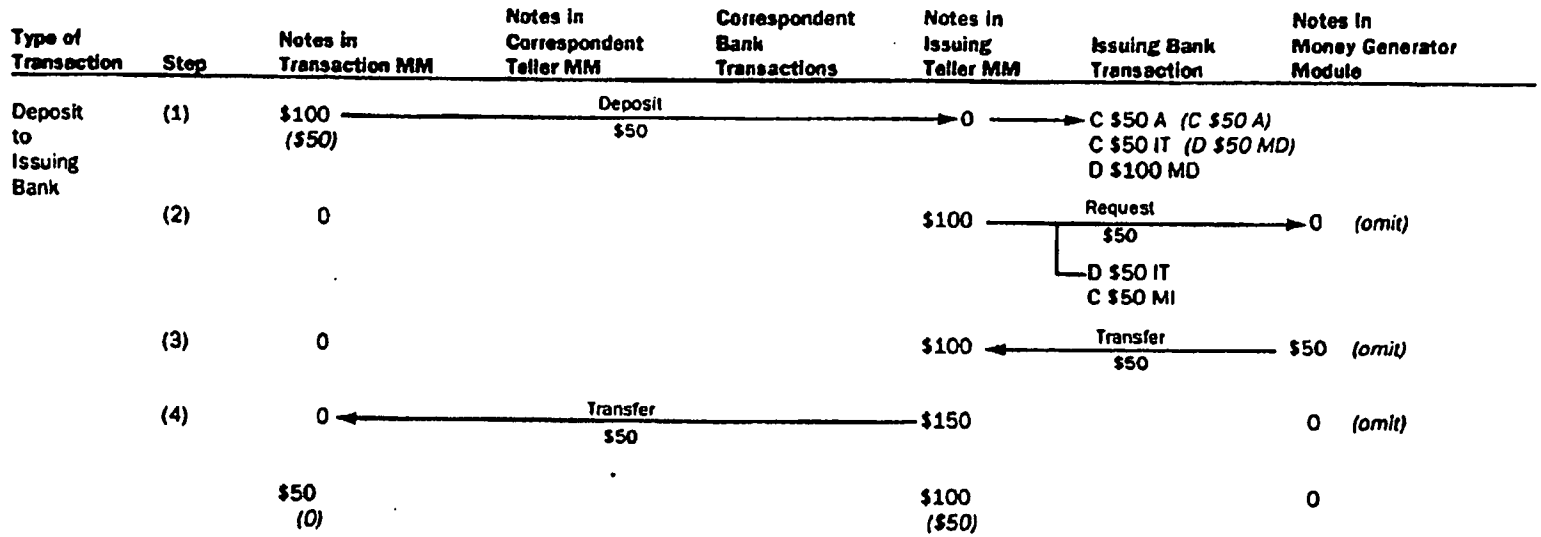
FIG. 11



Key: ( ) — Alternate values and steps

EP 0 542 298 B1

FIG. 12



Key: ( ) — Alternate values and steps

EP 0 542 298 B1

FIG. 13

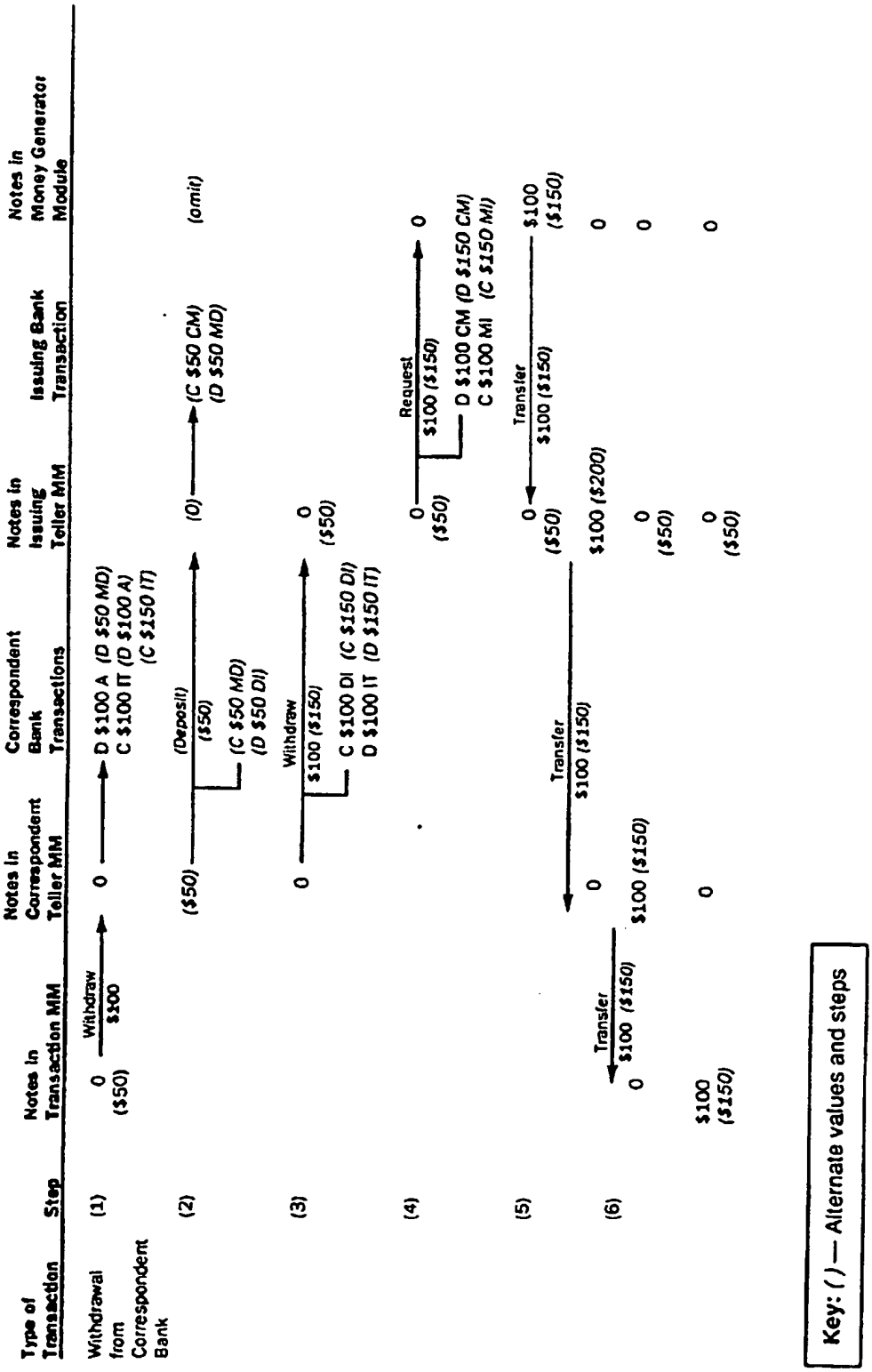
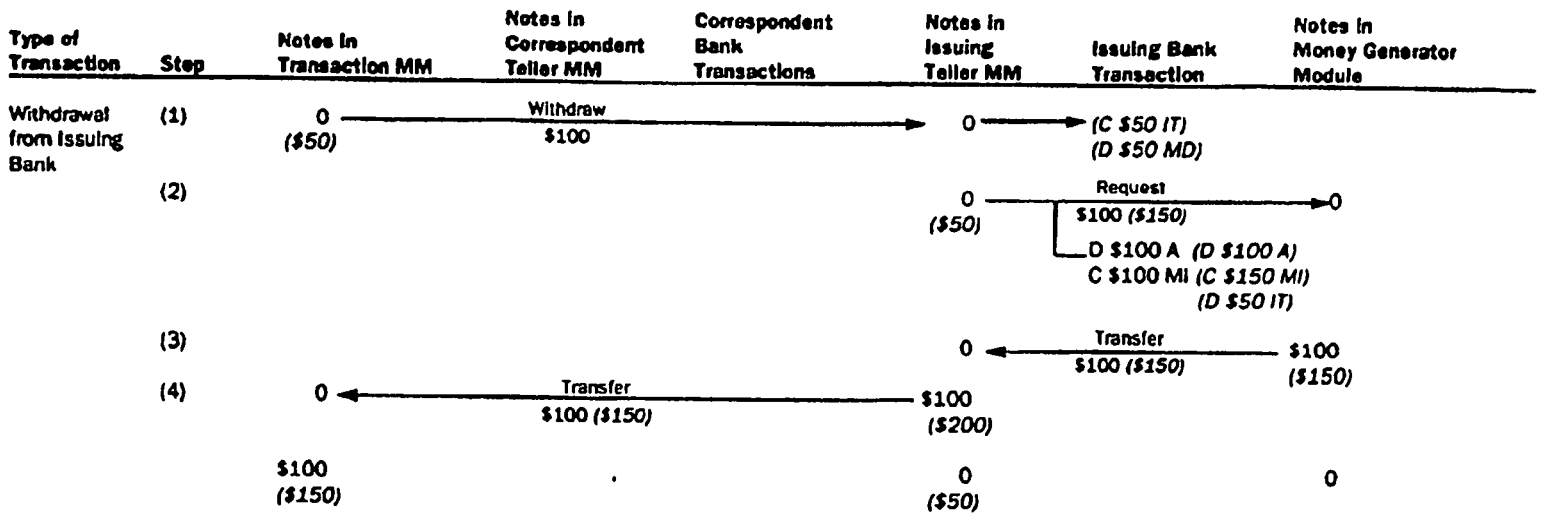

Type of Transaction
Step
Notes in Transaction MM
Notes in Correspondent Teller MM
Correspondent Bank Transactions
Notes in Issuing Teller MM
Issuing Bank Transaction
Notes in Money Generator Module
Withdrawal from Correspondent Bank
(1)
Withdraw
0
($50)
$100
0
D $100 A (D $50 MD)
C $100 IT (D $100 A)
(C $150 IT)
(2)
(Deposit)
($50)
($50)
(C $50 MD)
(D $50 DI)
(0)
(C $50 CM)
(D $50 MD)
(omit)
(3)
Withdraw
0
$100 ($150)
0
($50)
C $100 DI (C $150 DI)
D $100 IT (D $150 IT)
(4)
Request
0
($50)
$100 ($150)
0
D $100 CM (D $150 CM)
C $100 MI (C $150 MI)
(5)
Transfer
0
($50)
$100 ($150)
$100
($150)
Transfer
0
$100 ($150)
$100 ($150)
$100 ($200)
0
(6)
Transfer
0
$100 ($150)
$100 ($150)
0
($50)
0
$100
($150)
0
0
($50)
0
Key: ( ) — Alternate values and steps

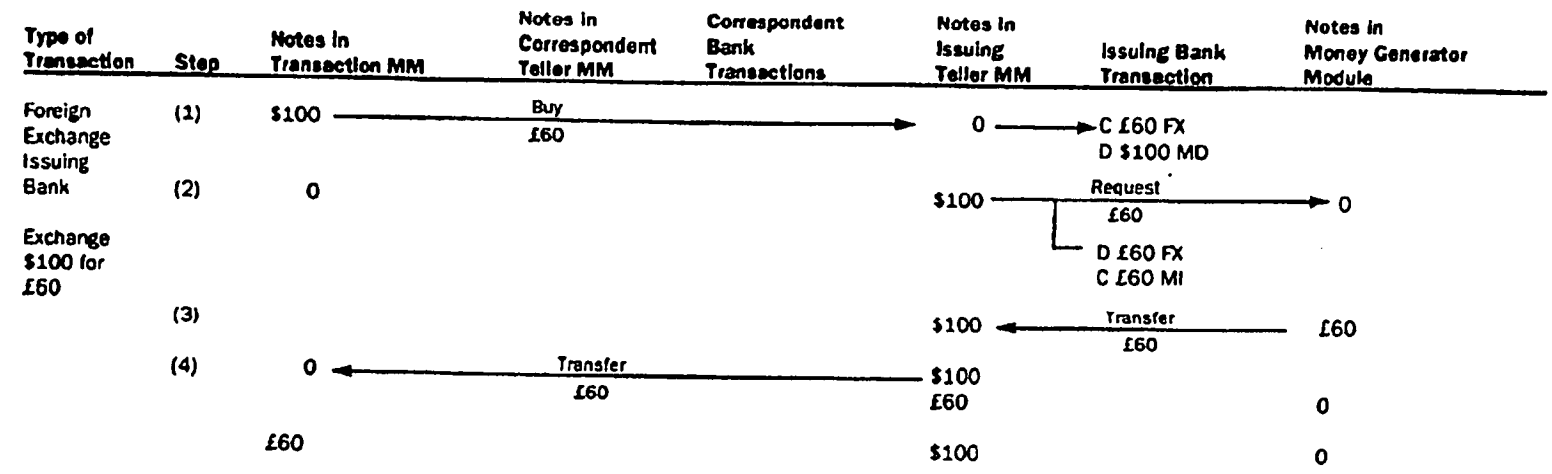
FIG. 14



Key: ( ) — Alternate values and steps

EP 0 542 298 B1

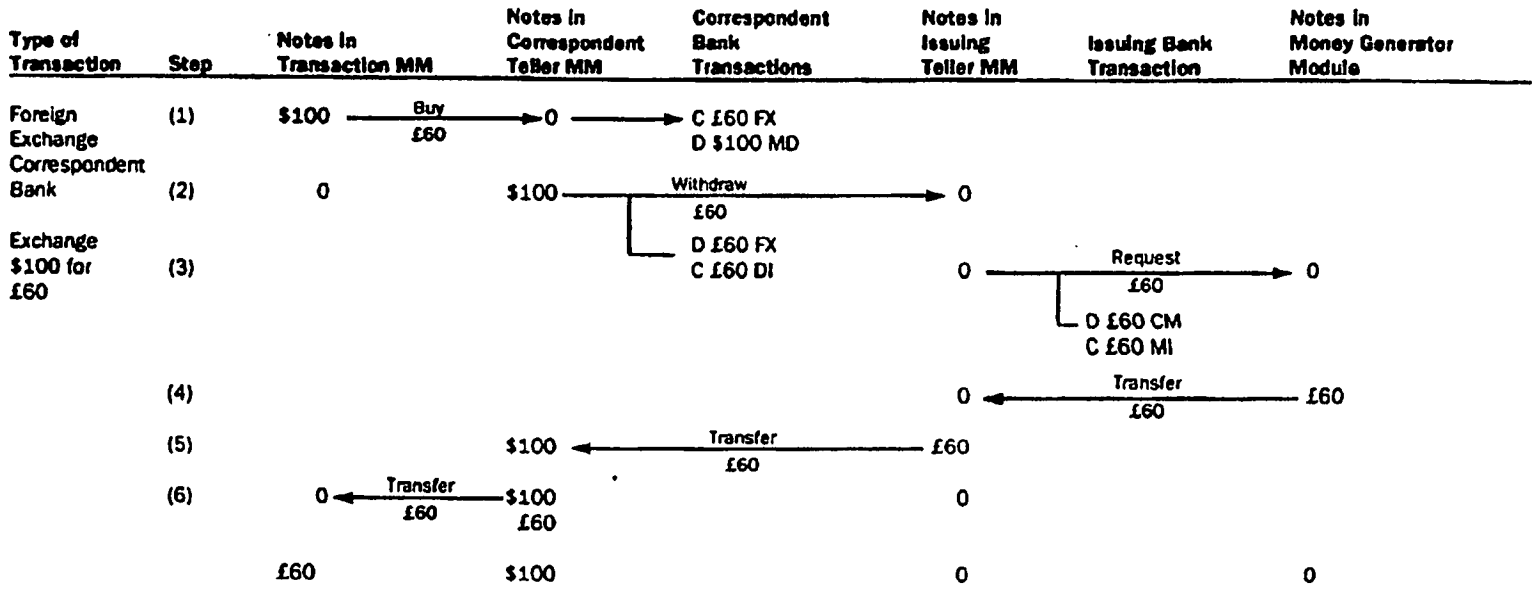
FIG. 15



Key: ( ) — Alternate values and steps

EP 0 542 298 B1

FIG. 16



Key: ( ) — Alternate values and steps

EP 0 542 298 B1

FIG. 17

Type of Transaction	Step	Notes in Transaction MM	Notes in Teller MM'	Notes in Money Generator Module	Bank Transaction
Withdraw Credit Notes	(1)	0 ← Withdraw $100 CR	0		→ Reduce Subscribers' Available Credit lin by $100
	(2)		0 → Request $100 CR	0	
	(3)		0 ← Transfer $100 CR	$100 CR	
	(4)	0 ← Transfer $100 CR	$100 CR		
		$100 CR	0	0	
Deposit Credit Notes	(1)	$50 CR → Deposit $50 CR	0		→ C $50 A D $50 MD
		0	$50		

Key: ( ) — Alternate values and steps

EP 0 542 298 B1

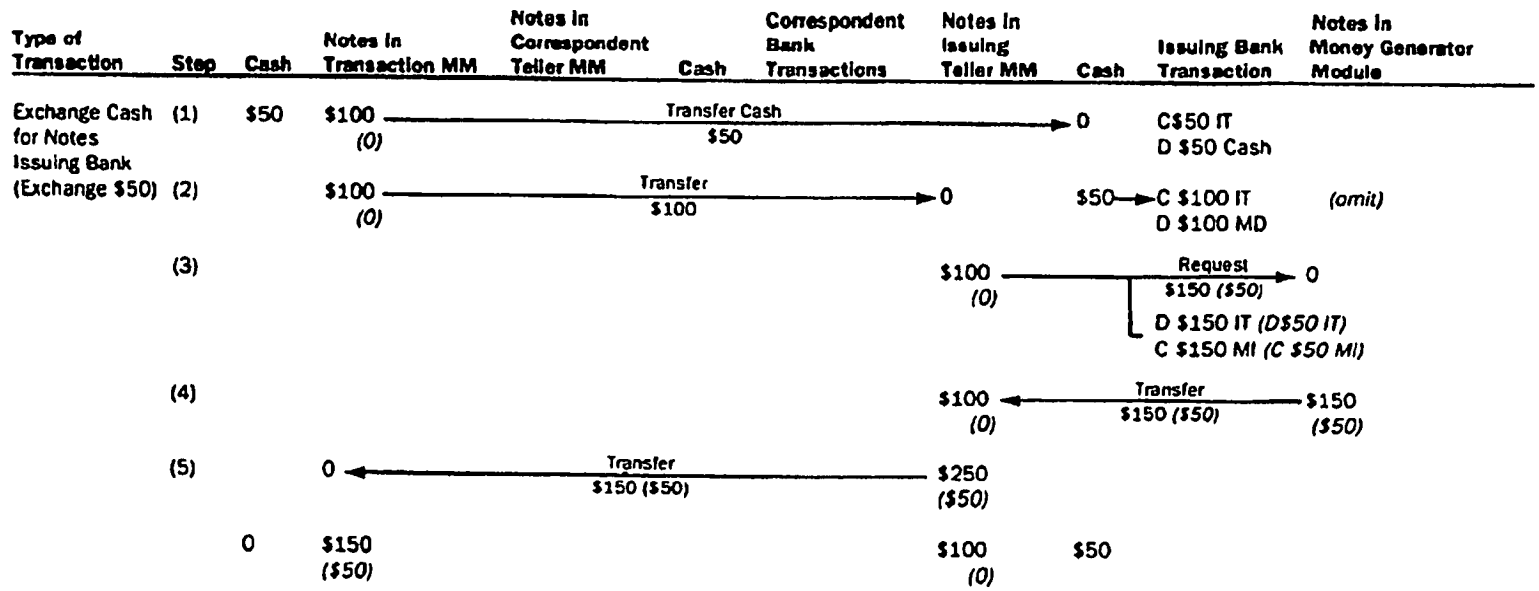
FIG. 18

Type of Transaction	Step	Clearing Bank		Issuing Bank	Accounting Transaction
Transfer notes from Clearing Bank to Issuing Bank	(1)	$100 $100 CR (on account A)	Transfer notes →	$50 (Deposited at Issuing Bank) 0	D $100 A D $150 MI C $50 MD C $200 DC
		0		$150 $100 CR	

Key: ( ) — Alternate values and steps

EP 0 542 298 B1

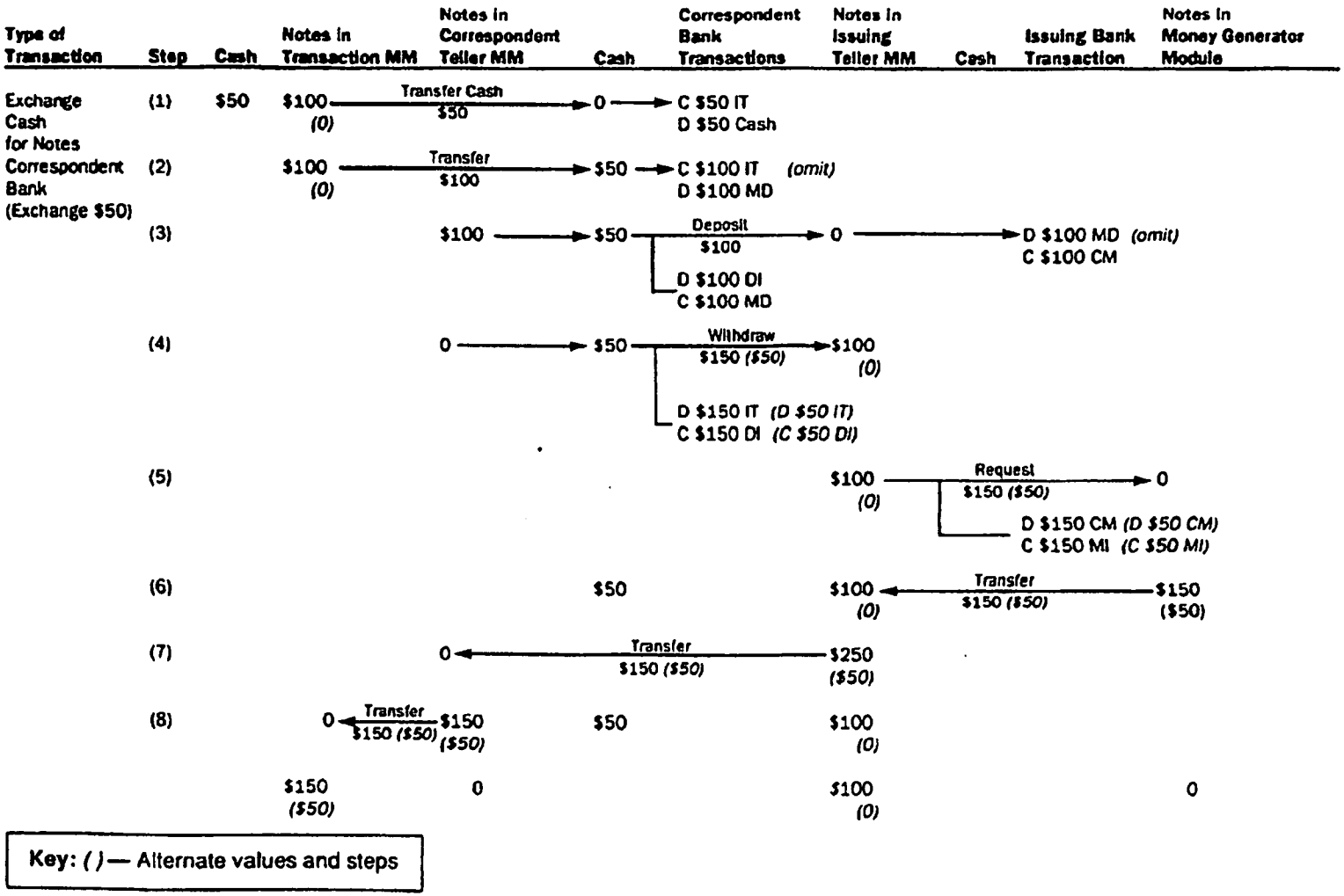
FIG. 19



Key: ( ) — Alternate values and steps

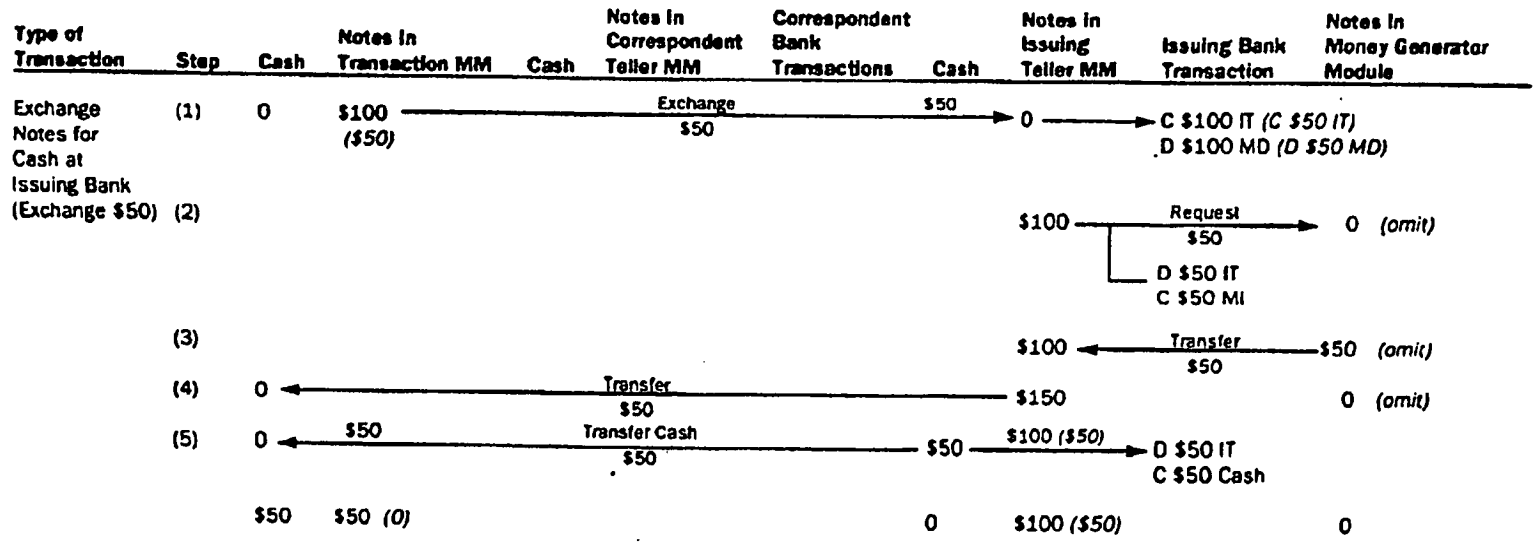
EP 0 542 298 B1

FIG. 20



EP 0 542 298 B1

FIG. 21



Key: ( ) — Alternate values and steps

FIG. 22

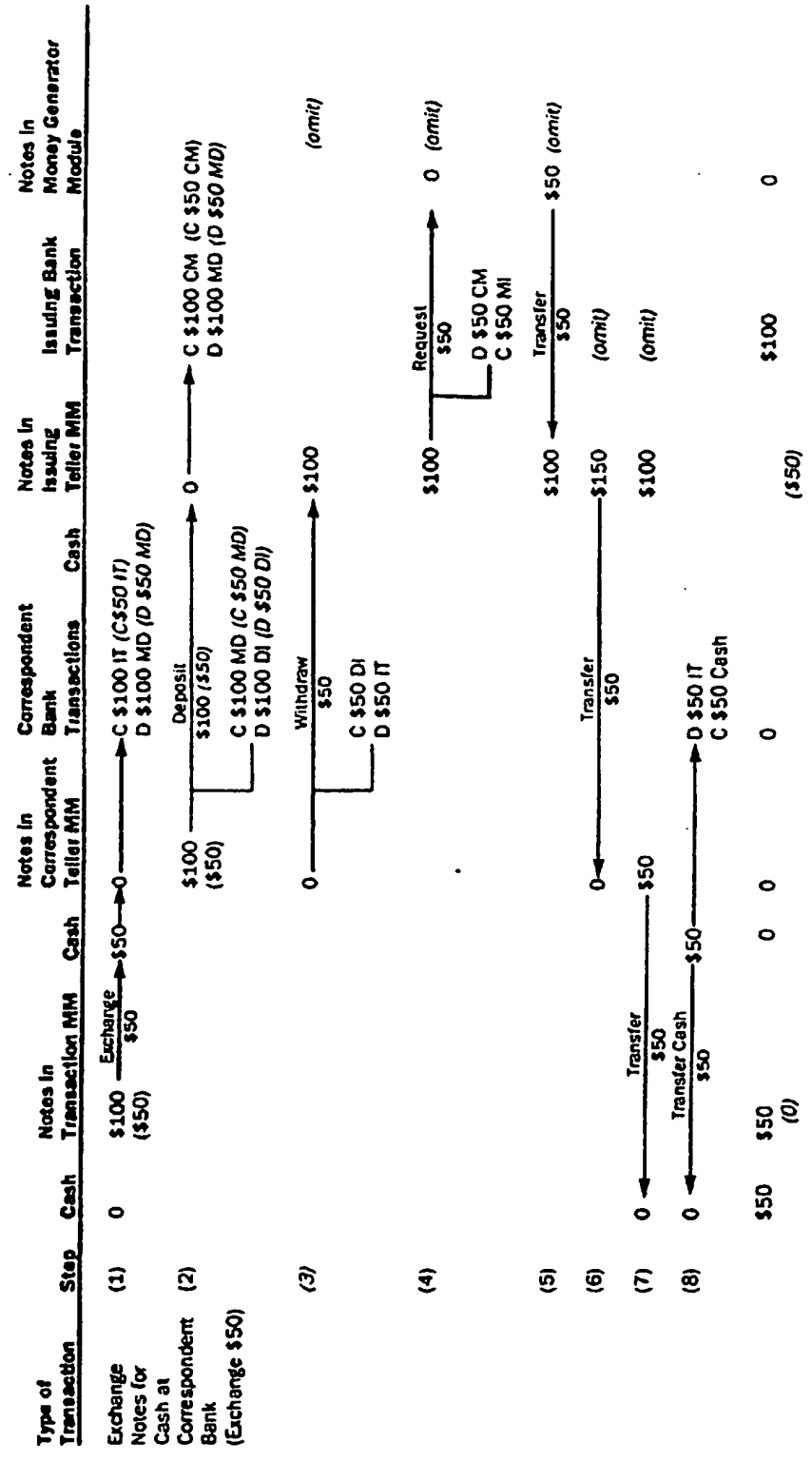
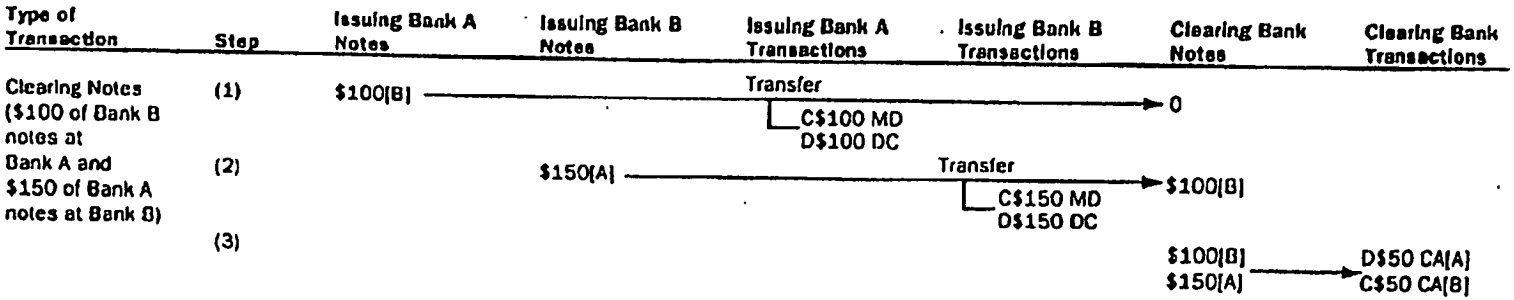

Type of Transaction
Step
Cash
Notes in Transaction MM
Cash
Notes in Correspondent Teller MM
Correspondent Bank Transactions
Cash
Notes in Issuing Teller MM
Issuing Bank Transaction
Notes in Money Generator Module
Exchange Notes for Cash at Correspondent Bank (Exchange $50)
(1)
0
$100 ($50)
Exchange
$50
$50
0
C $100 IT (C$50 IT)
D $100 MD (D $50 MD)
(2)
$100 ($50)
Deposit
$100 ($50)
0
C $100 CM (C $50 CM)
D $100 MD (D $50 MD)
C $100 MD (C $50 MD)
D $100 DI (D $50 DI)
(3)
Withdraw
$50
0
$100
(omit)
C $50 DI
D $50 IT
(4)
$100
Request
$50
0
(omit)
D $50 CM
C $50 MI
(5)
$100
Transfer
$50
$50
(omit)
(6)
Transfer
$50
0
$150
(omit)
(7)
0
Transfer
$50
$50
$100
(omit)
(8)
0
Transfer Cash
$50
$50
D $50 IT
C $50 Cash
$50
$50
(0)
0
0
0
($50)
$100
0
Key: ( ) — Alternate values and steps

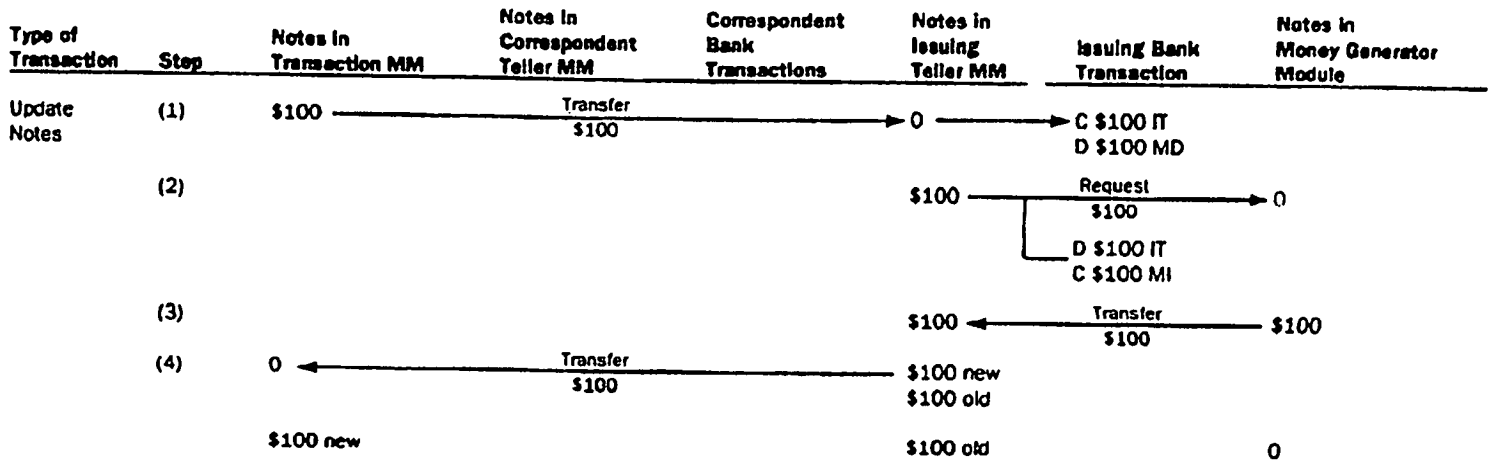
FIG. 23



Key: ( ) — Alternate values and steps

EP 0 542 298 B1

FIG. 24



Key: ( ) — Alternate values and steps

EP 0 542 298 B1

FIG. 25

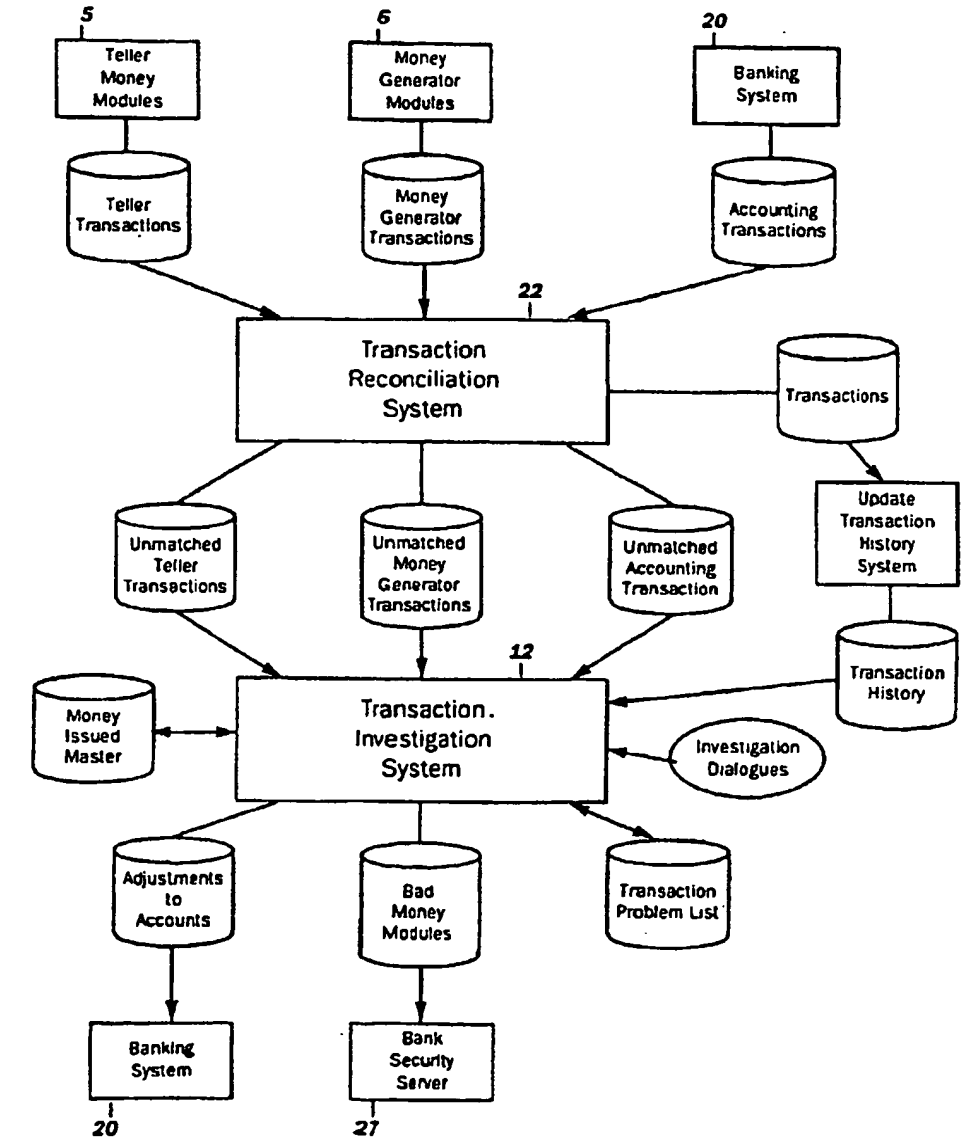
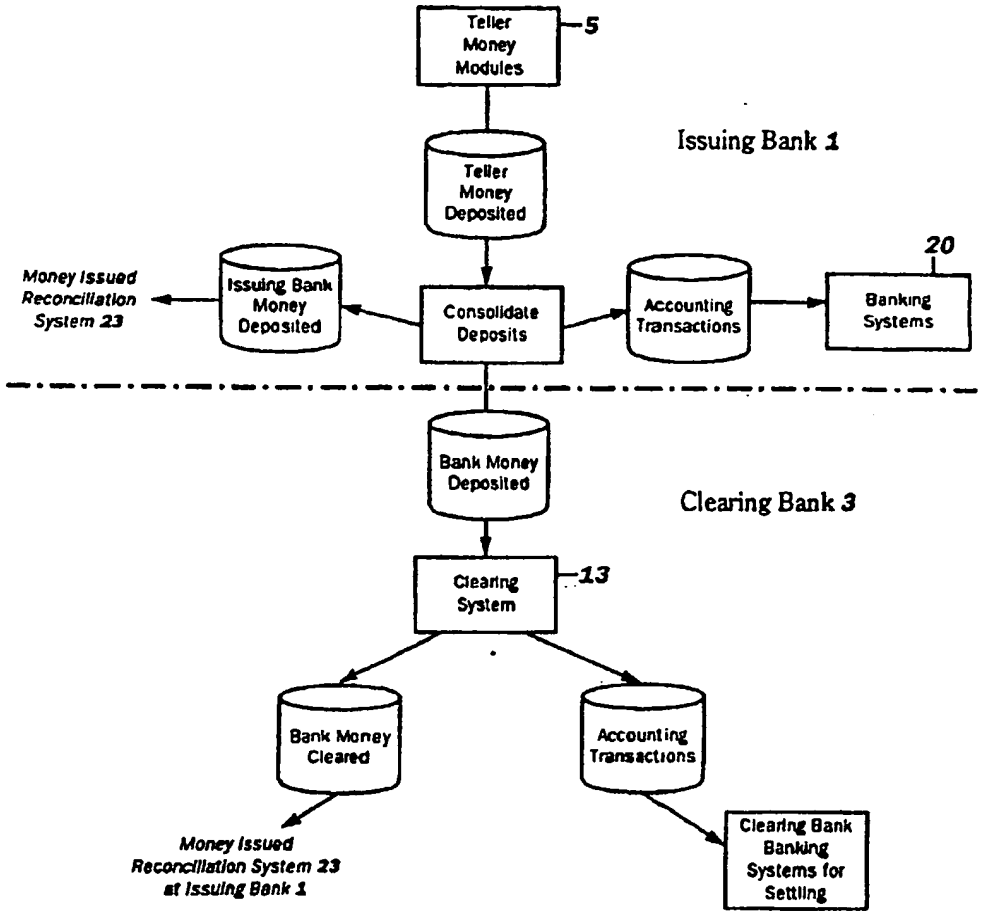
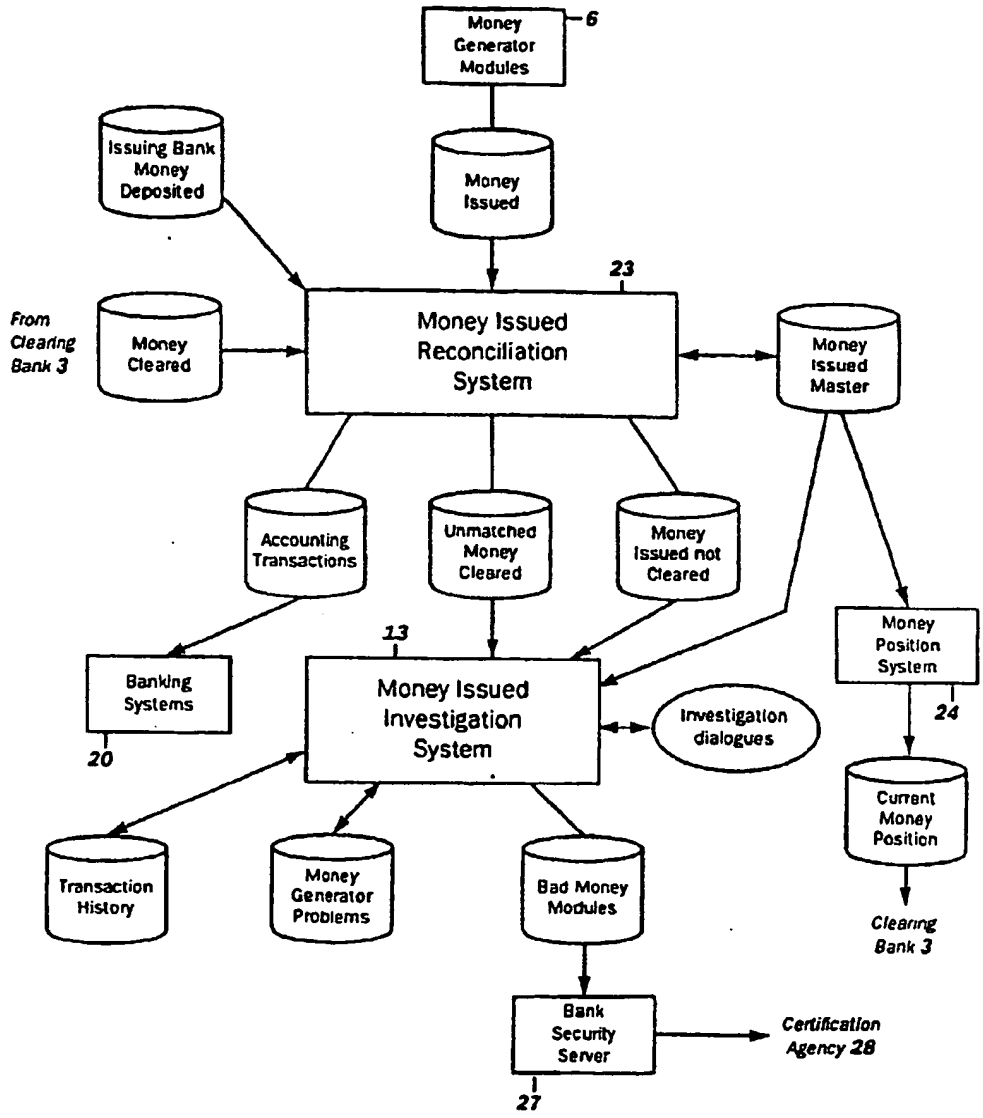

5
Teller Money Modules
6
Money Generator Modules
20
Banking System
Teller Transactions
Money Generator Transactions
Accounting Transactions
22
Transaction Reconciliation System
Transactions
Update Transaction History System
Unmatched Teller Transactions
Unmatched Money Generator Transactions
Unmatched Accounting Transaction
12
Transaction History
Money Issued Master
Transaction. Investigation System
Investigation Dialogues
Adjustments to Accounts
Bad Money Modules
Transaction Problem List
Banking System
Bank Security Server
20
27
Transaction Reconciliation System

FIG. 26



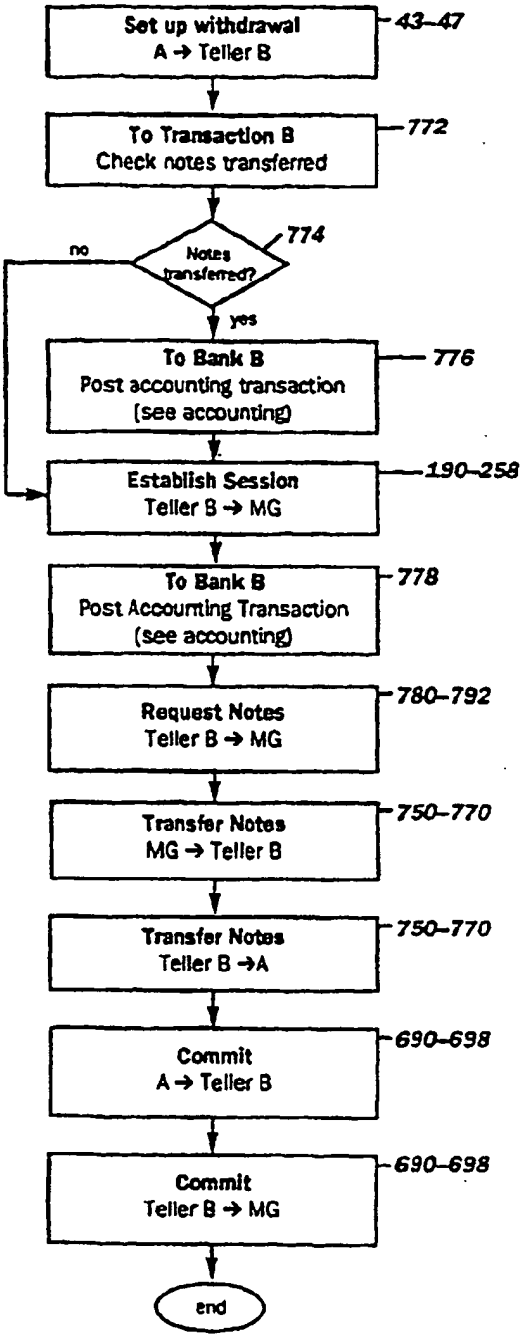
Clearing System

FIG. 27



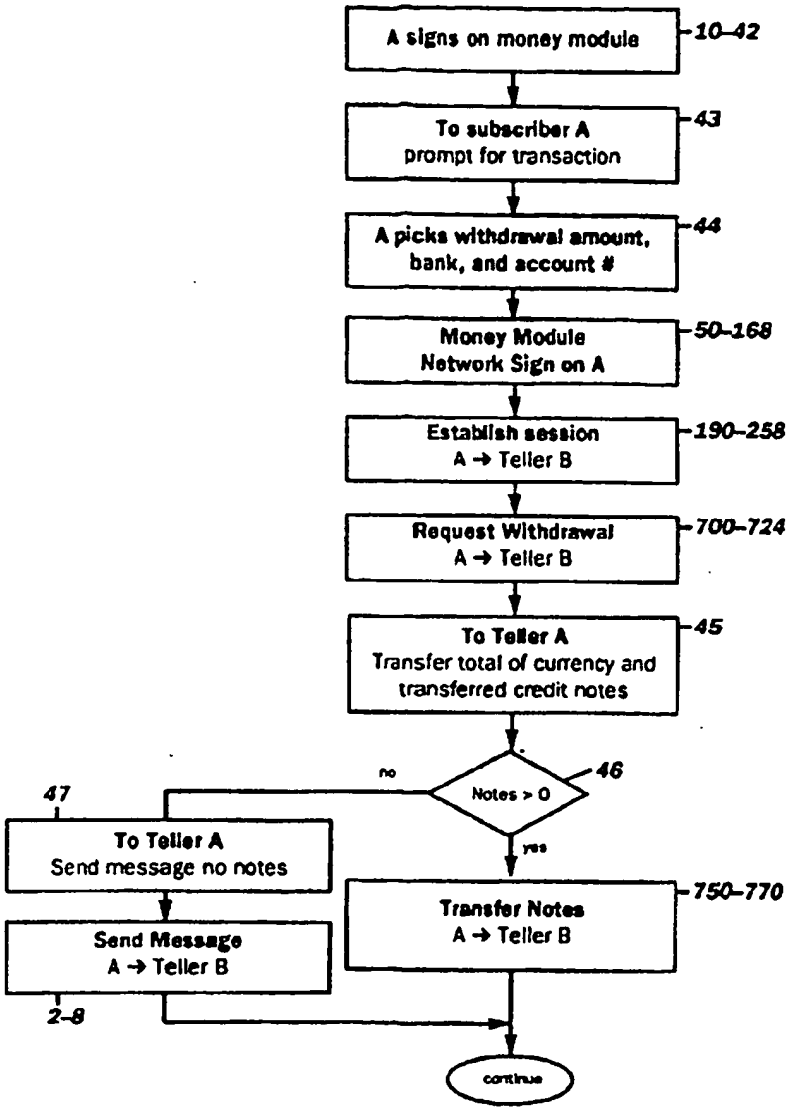
Money Issued Reconciliation System

FIG 28



Withdrawal from Issuing Bank

FIC. 29



Setup Withdrawal

FIG. 30

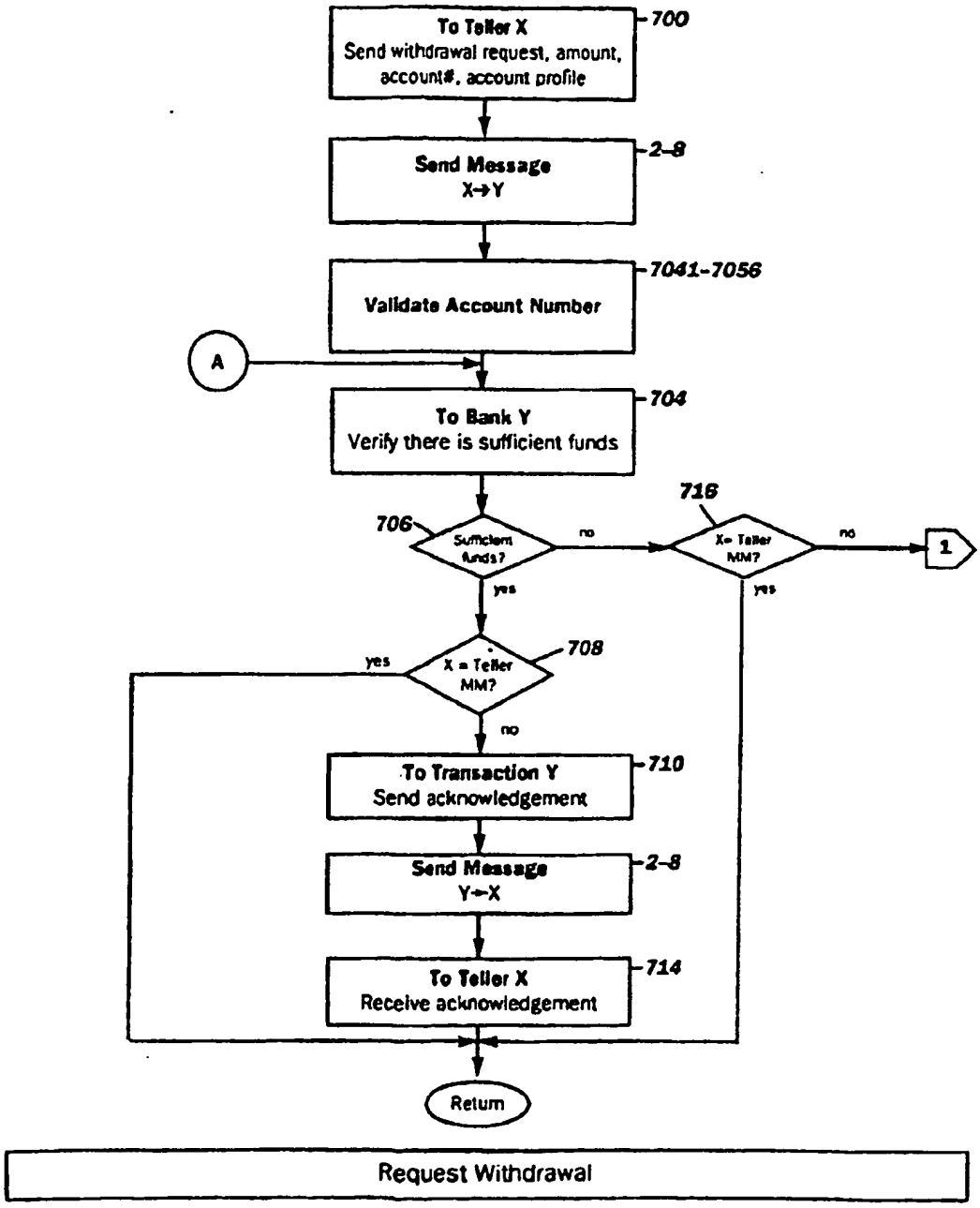
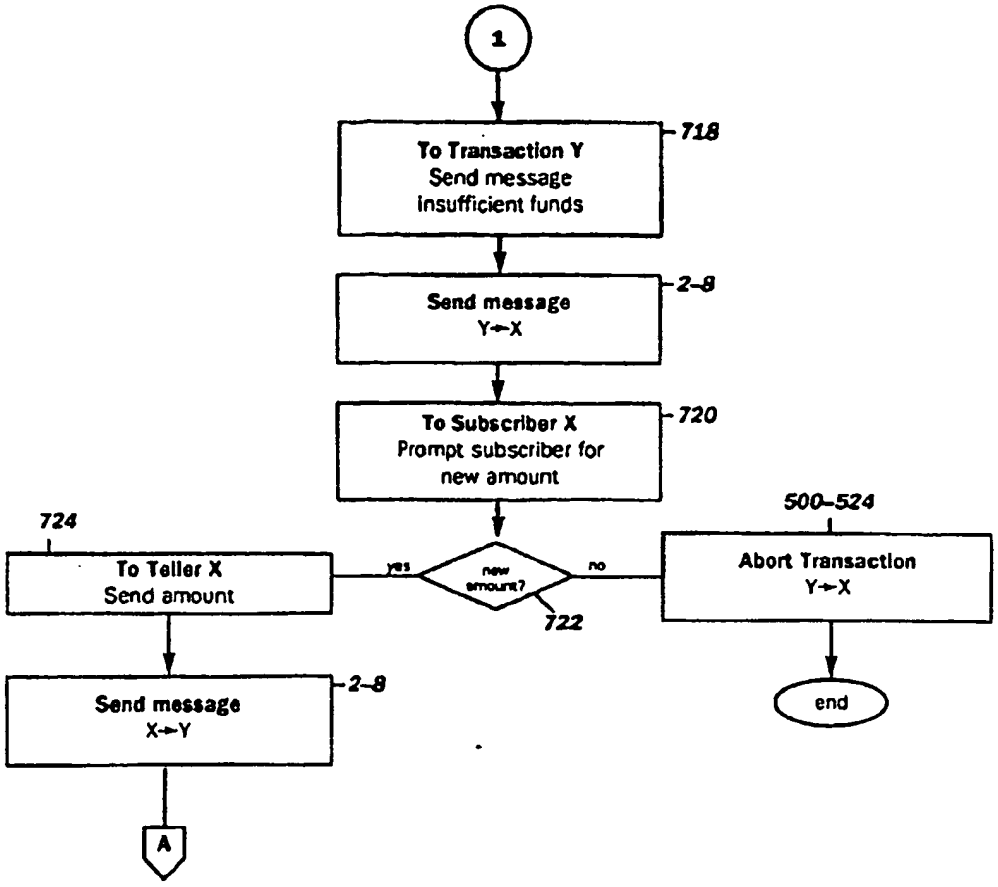
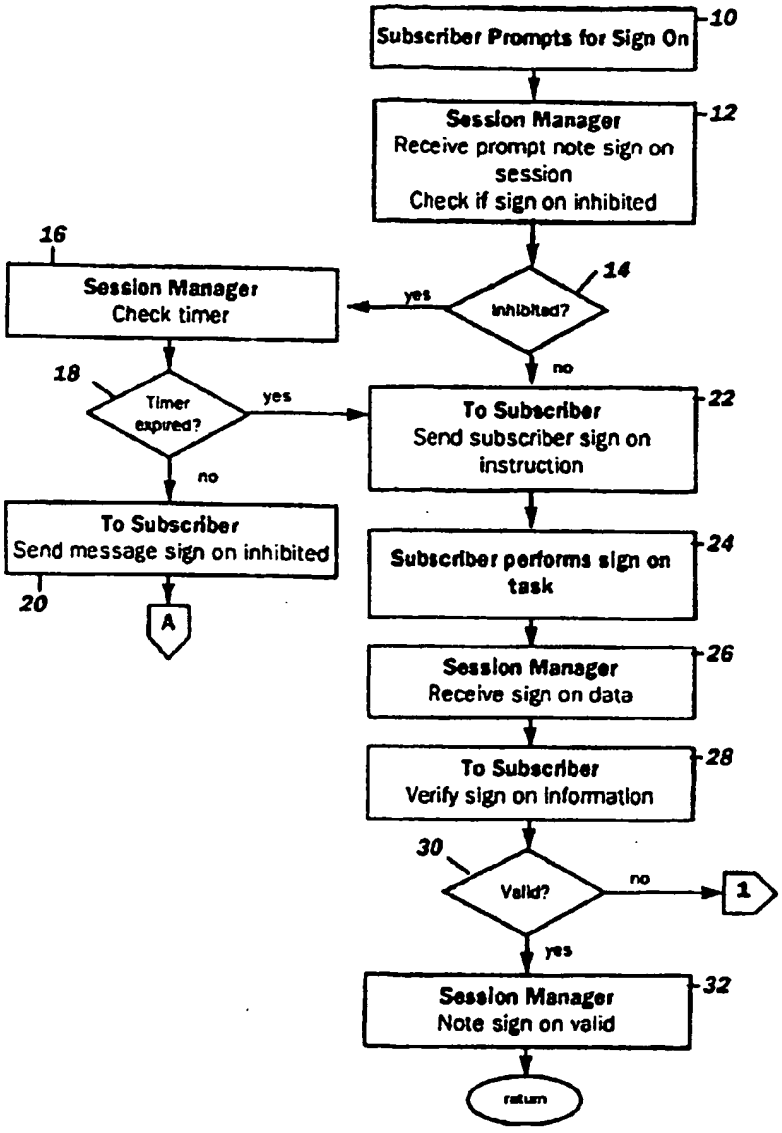

To Teller X
Send withdrawal request, amount, account#, account profile
700
Send Message
X→Y
2-8
Validate Account Number
7041-7056
A
To Bank Y
Verify there is sufficient funds
704
706
Sufficient funds?
no
716
X= Teller MM?
no
1
yes
yes
yes
X = Teller MM?
708
no
To Transaction Y
Send acknowledgement
710
Send Message
Y←X
2-8
To Teller X
Receive acknowledgement
714
Return
Request Withdrawal

FIG. 30A



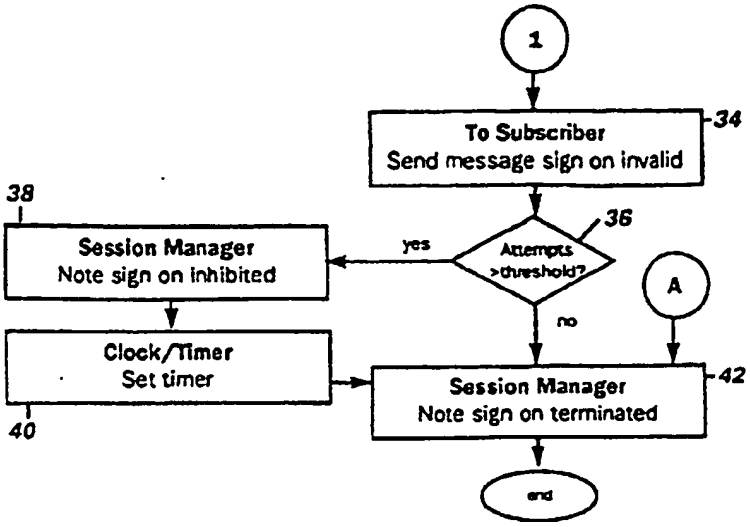
Request Withdrawal (continued)

FIG. 31



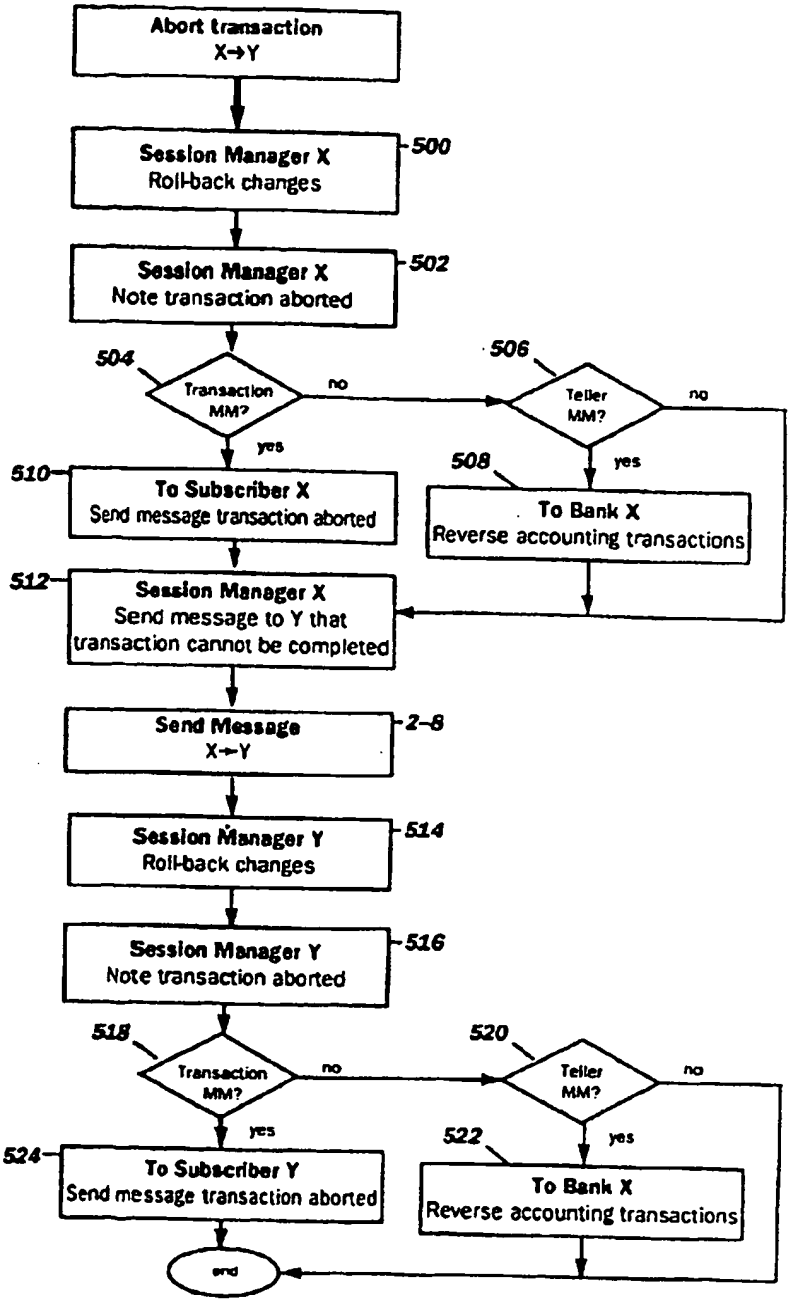
Subscriber Money Module Sign On

FIG. 31A



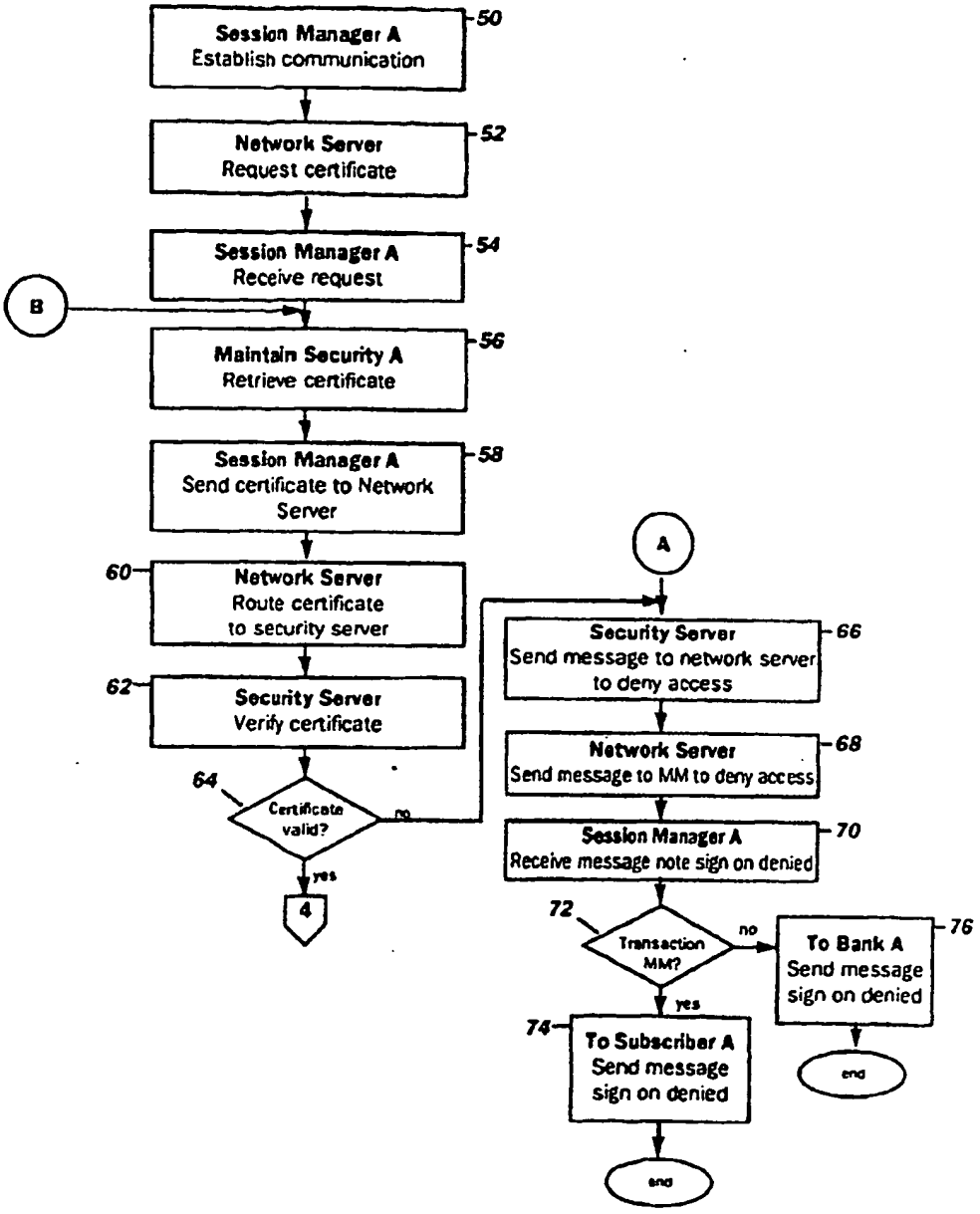
Subscriber Money Module Sign On (Continued)

FIG. 32



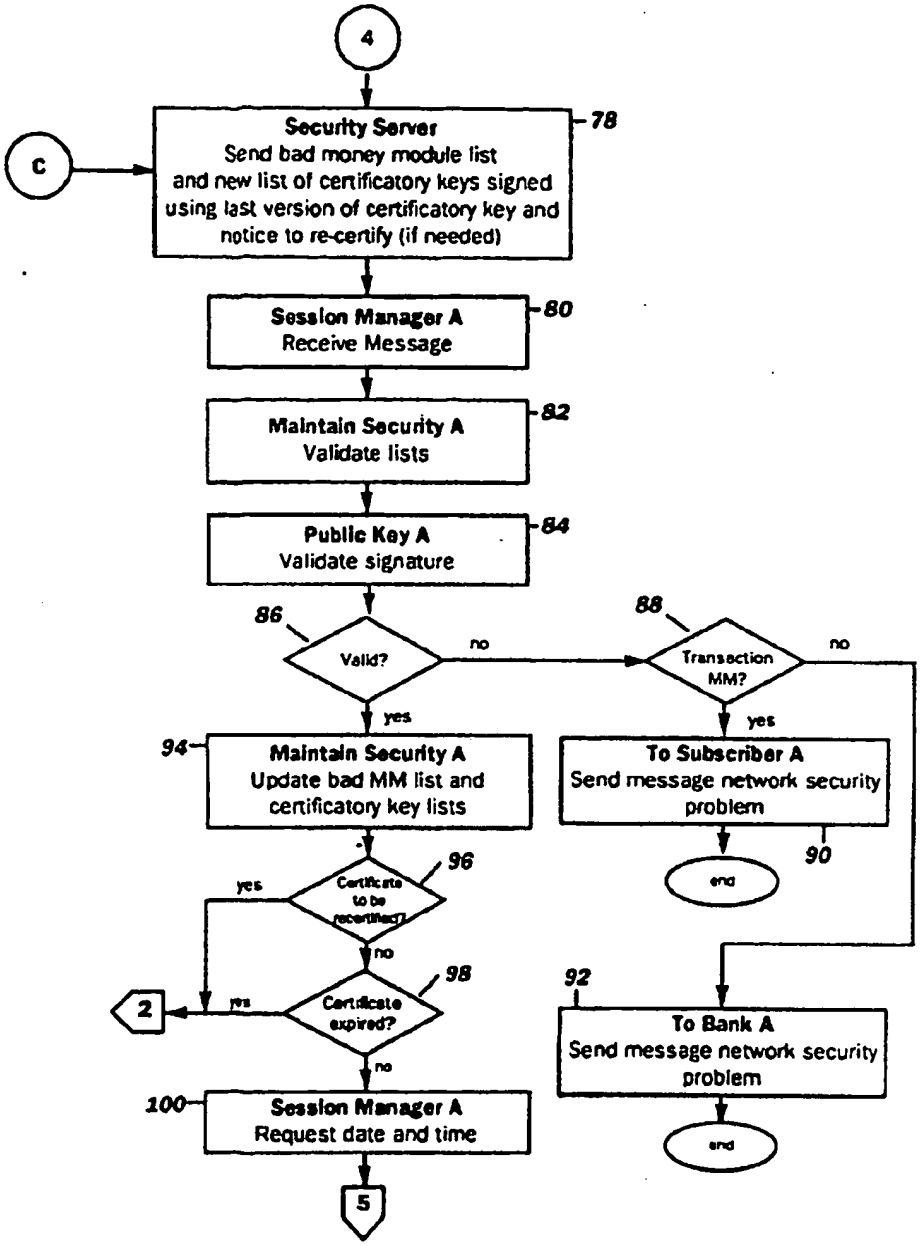
Abort Transaction Money Module to Money Module

FIG. 33



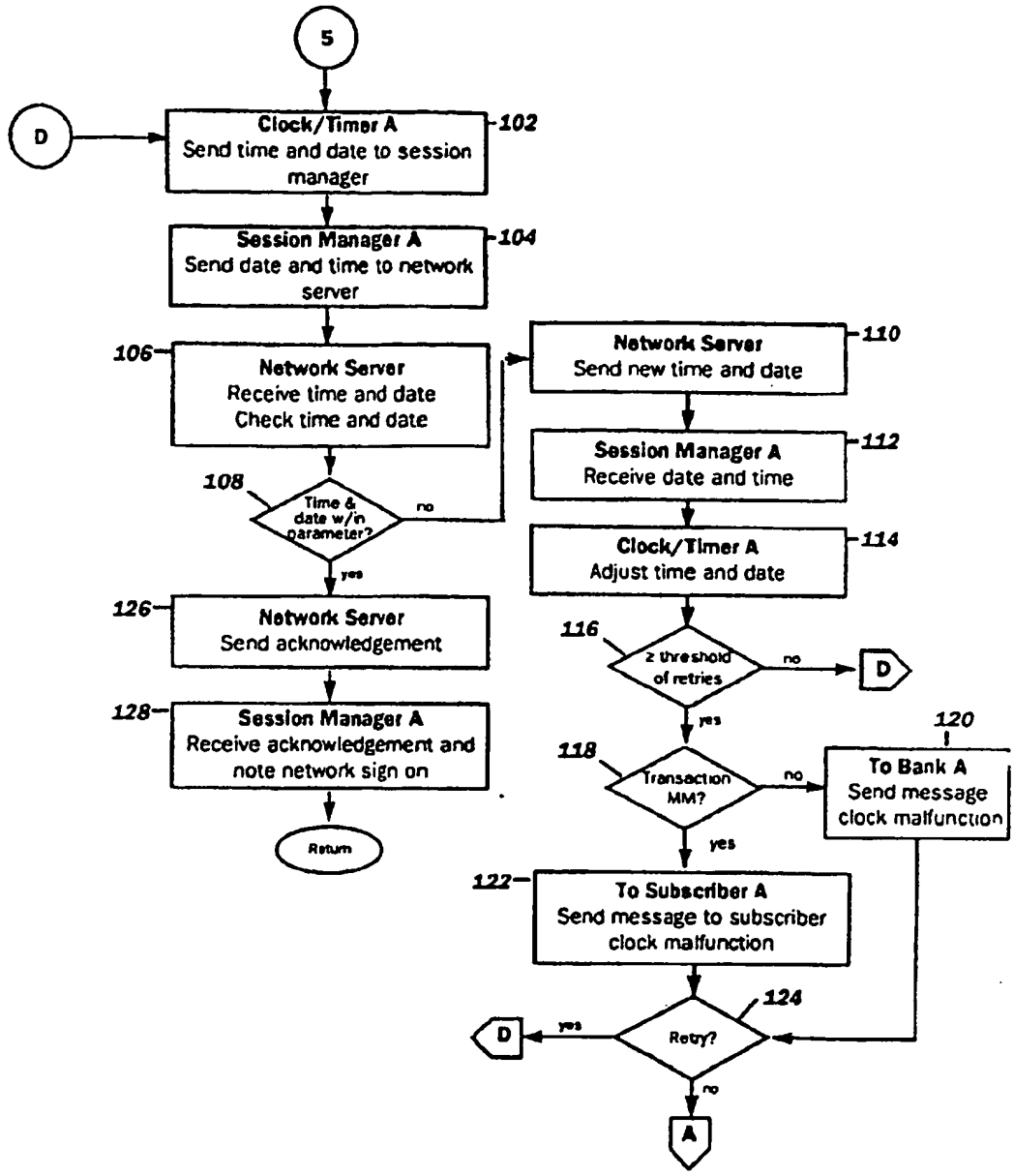
Money Module Network Sign On

FIG. 33A



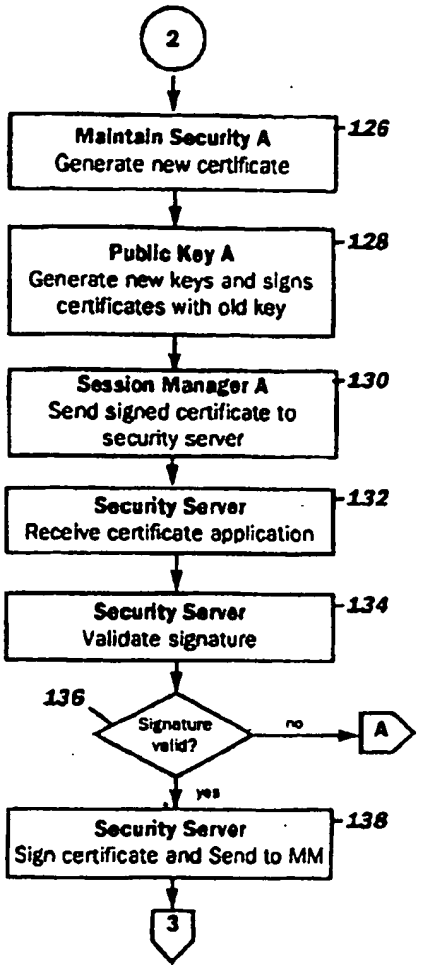
Money Module Network Sign On (continued)

FIG. 33B



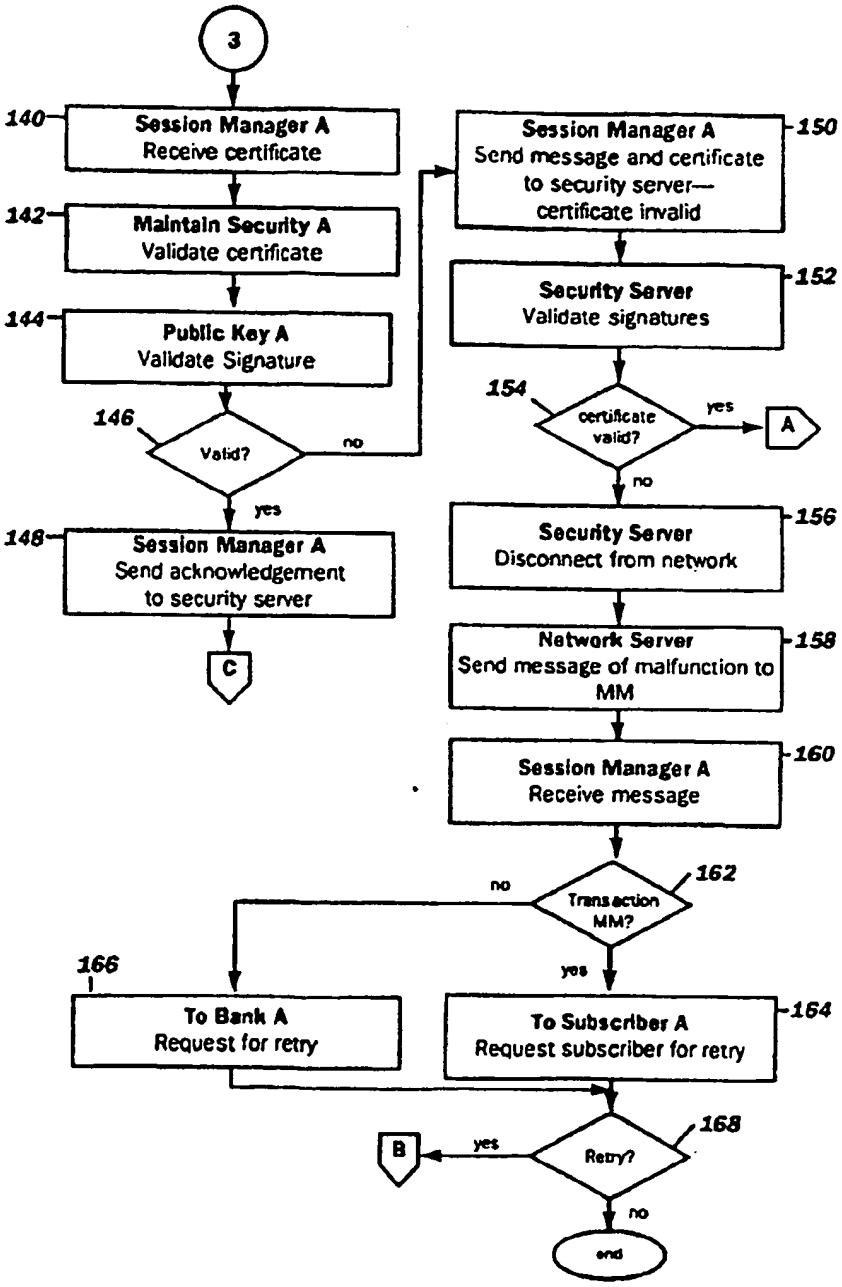
Money Module Network Sign On (continued)

FIG. 3C



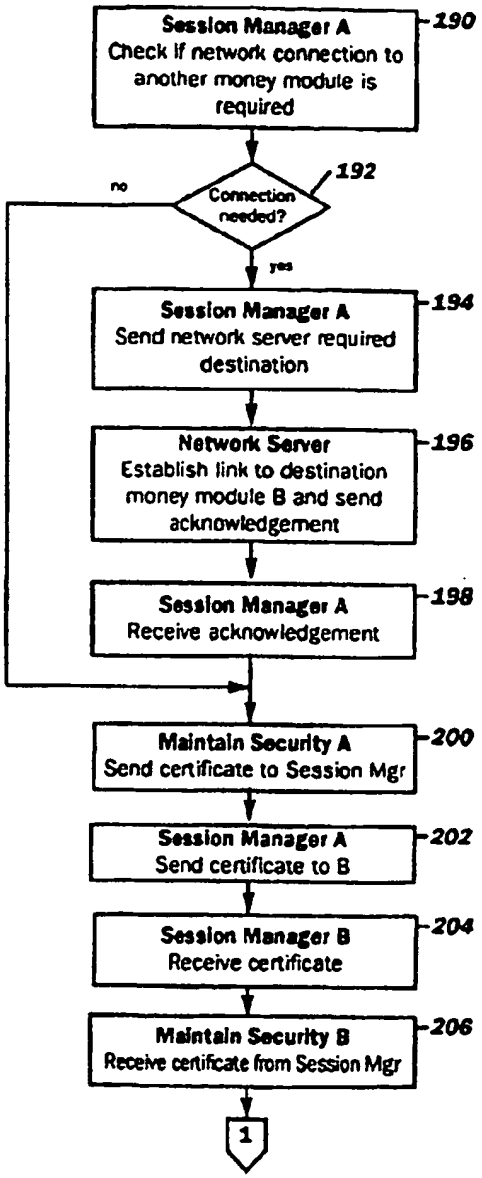
Money Module Network Sign On (continued)

FIG. 33D



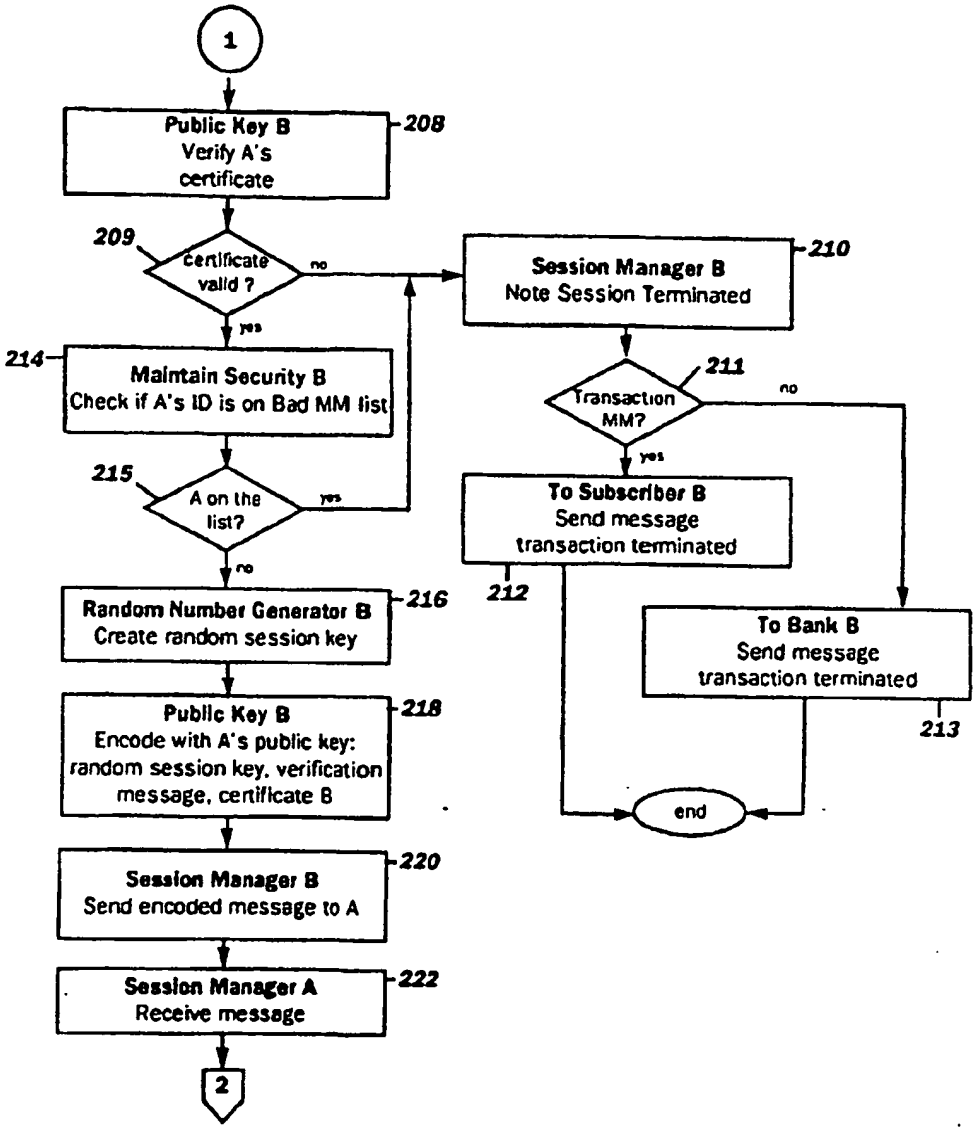
Money Module Network Sign On (continued)

FIG. 34



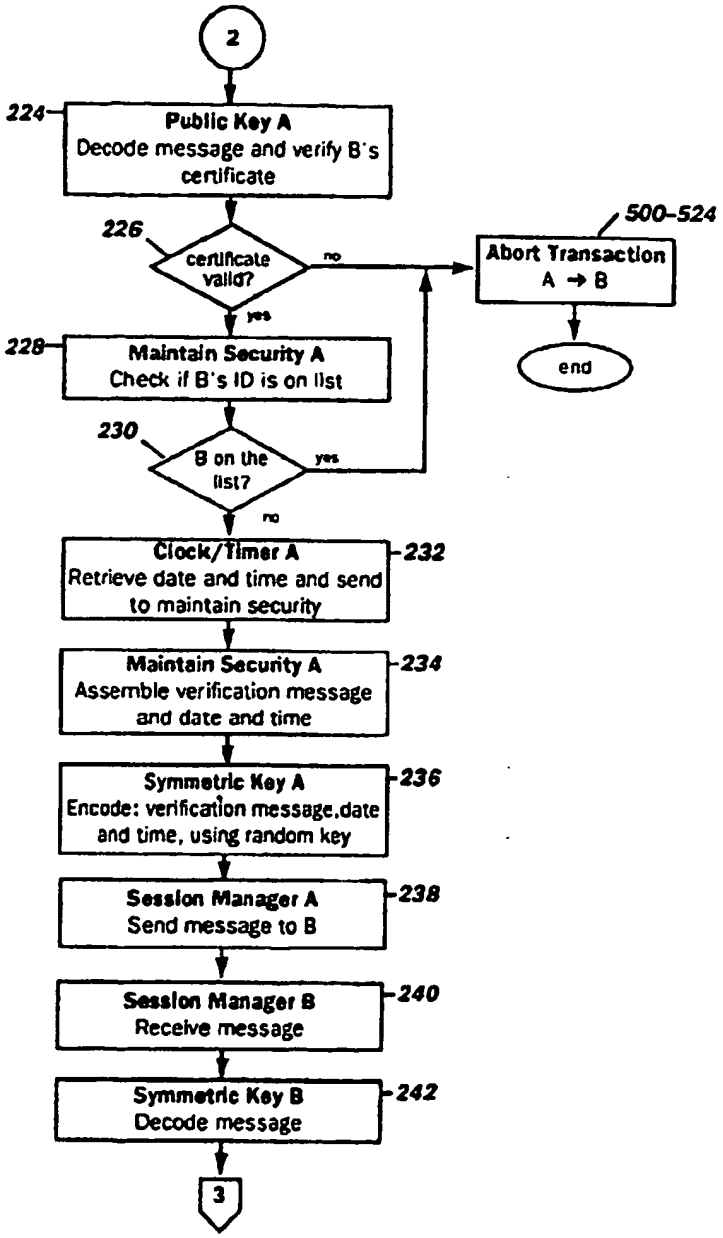
Establish Session — Money Module to Money Module

FIG. 34A



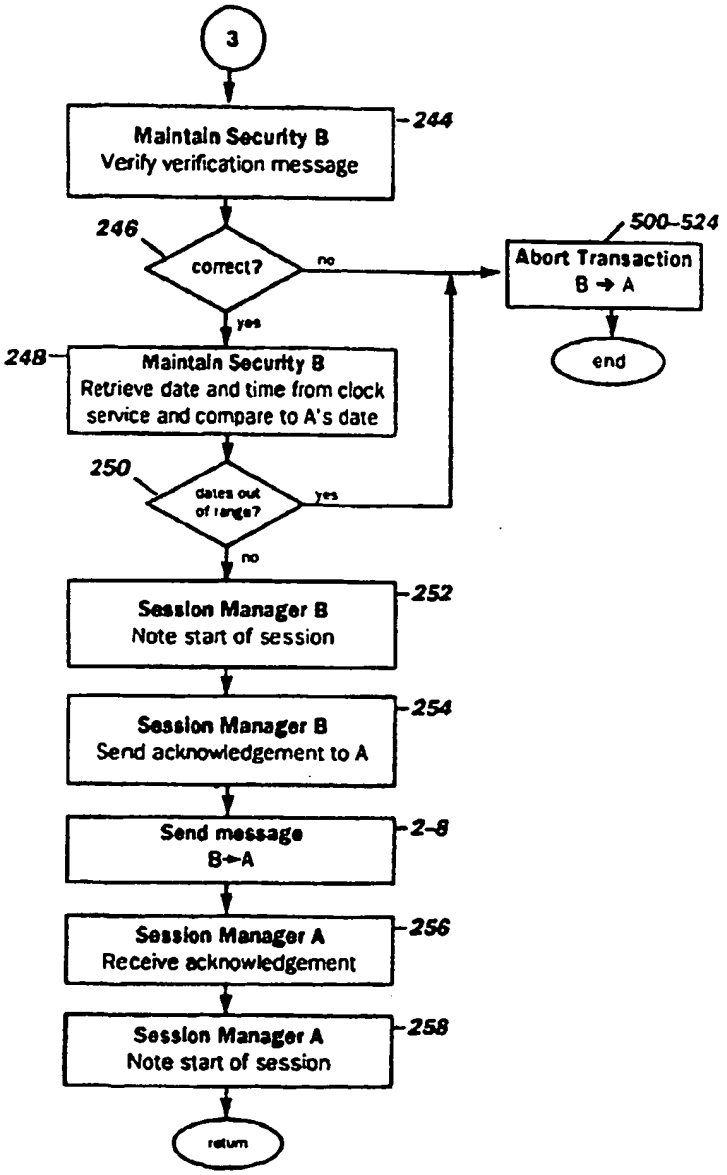
Establish Session — Money Module to Money Module (continued)

FIG. 34B



Establish Session — Money Module to Money Module (continued)

FIG. 34C



Establish Session — Money Module to Money Module (continued)

FIG 35

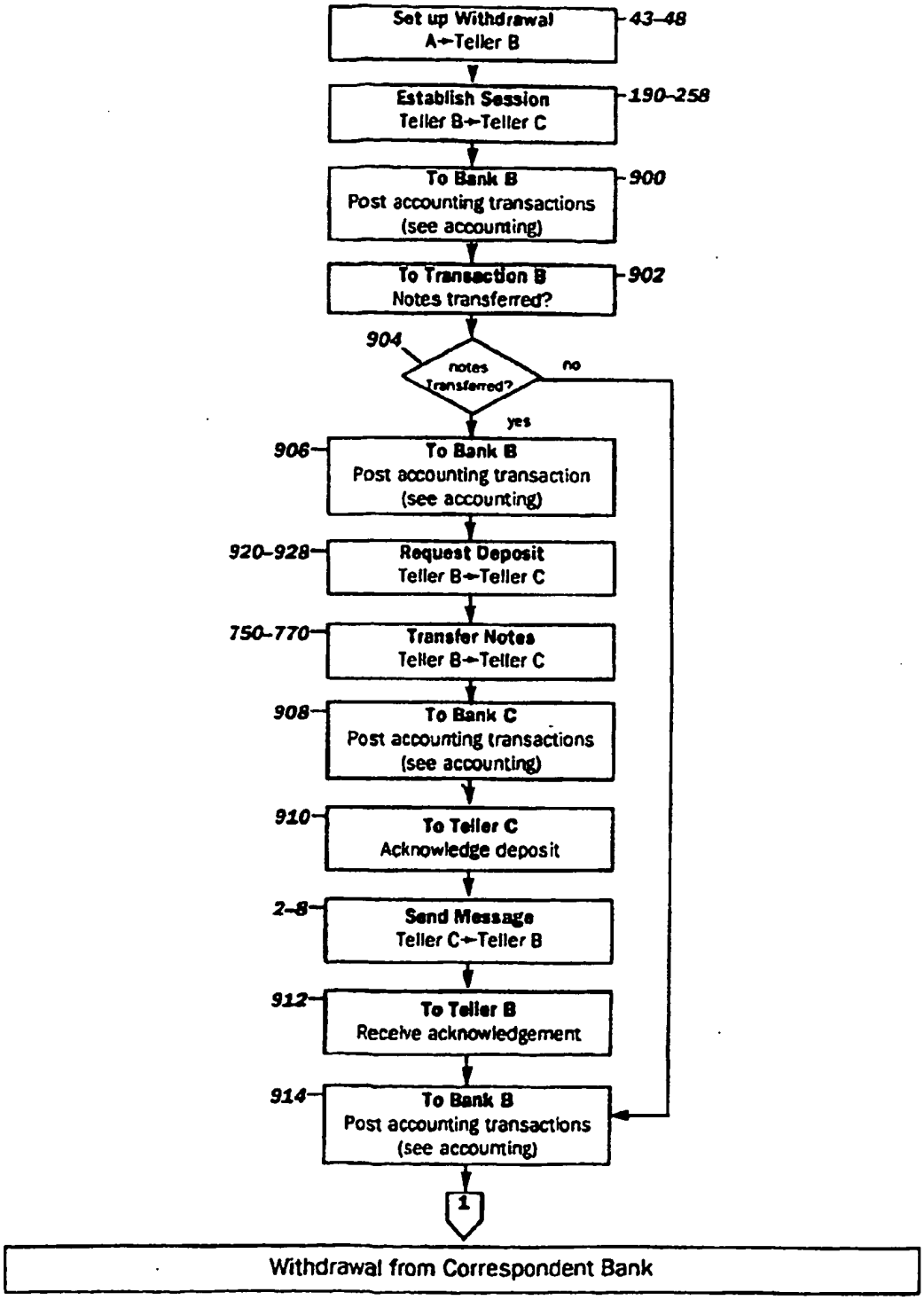
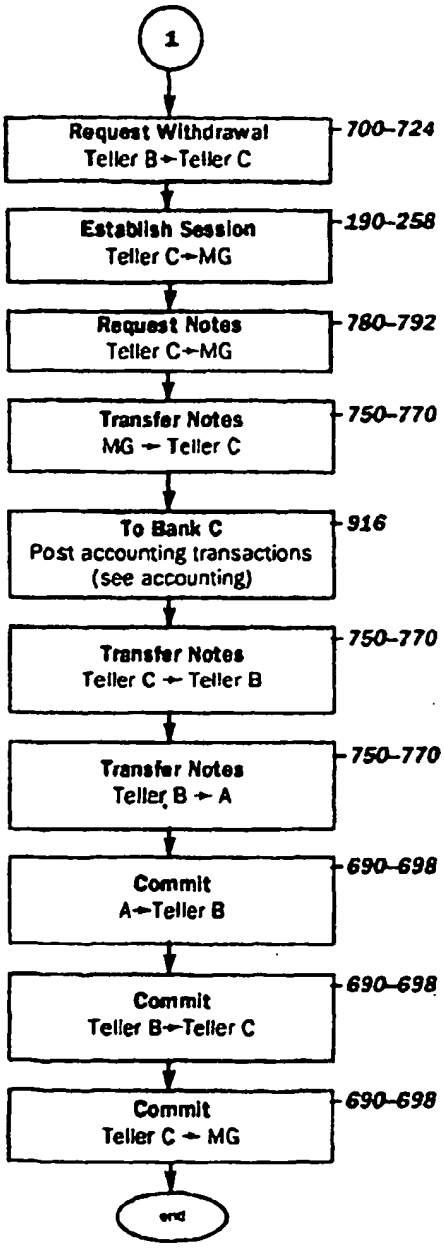

Set up Withdrawal
A←Teller B
43–48
Establish Session
Teller B←Teller C
190–258
To Bank B
Post accounting transactions
(see accounting)
900
To Transaction B
Notes transferred?
902
904
notes Transferred?
no
yes
906
To Bank B
Post accounting transaction
(see accounting)
920–928
Request Deposit
Teller B←Teller C
750–770
Transfer Notes
Teller B←Teller C
908
To Bank C
Post accounting transactions
(see accounting)
910
To Teller C
Acknowledge deposit
2–8
Send Message
Teller C←Teller B
912
To Teller B
Receive acknowledgement
914
To Bank B
Post accounting transactions
(see accounting)
1
Withdrawal from Correspondent Bank

FIG. 35A



Withdrawal from Correspondent Bank (continued)

FIG. 36

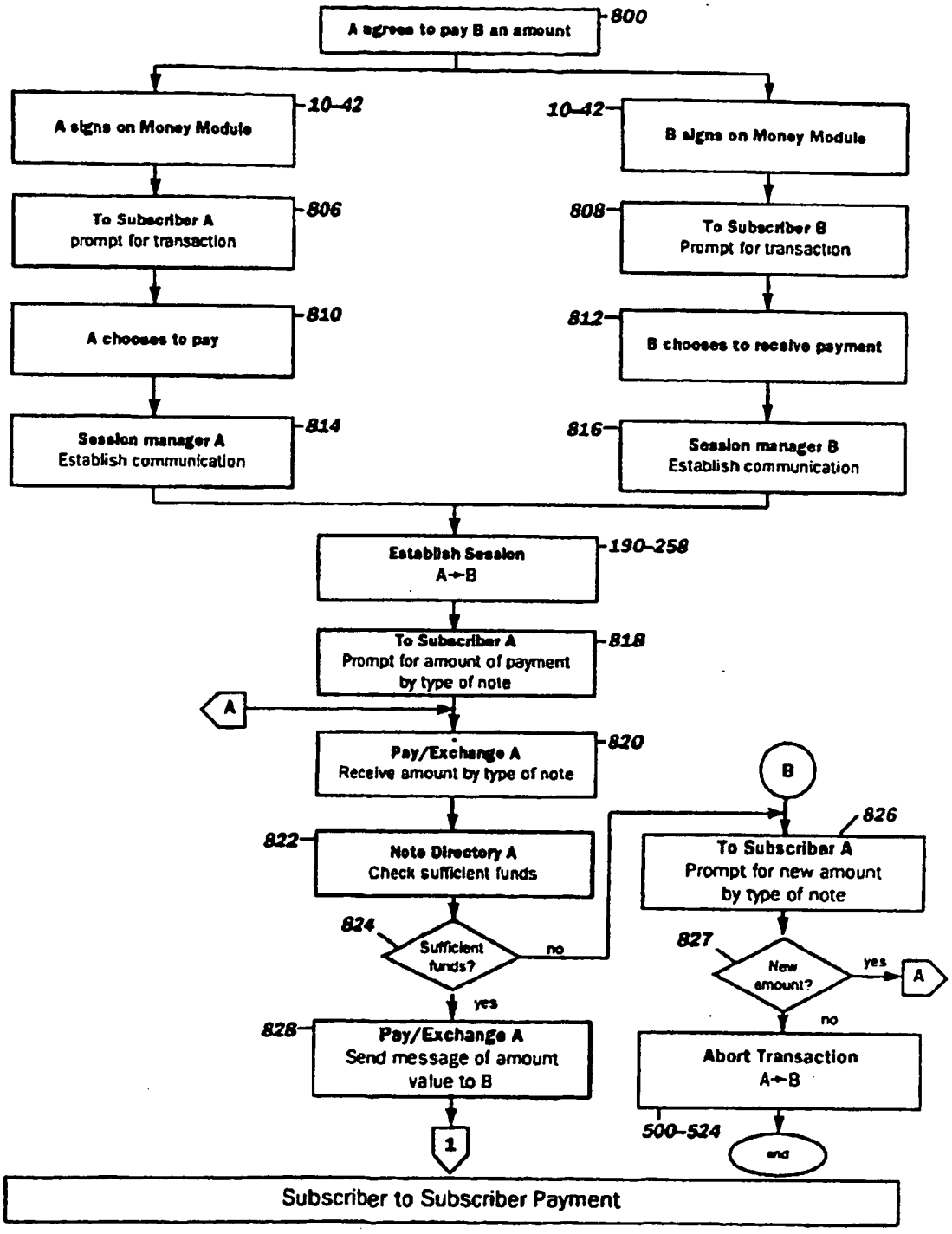
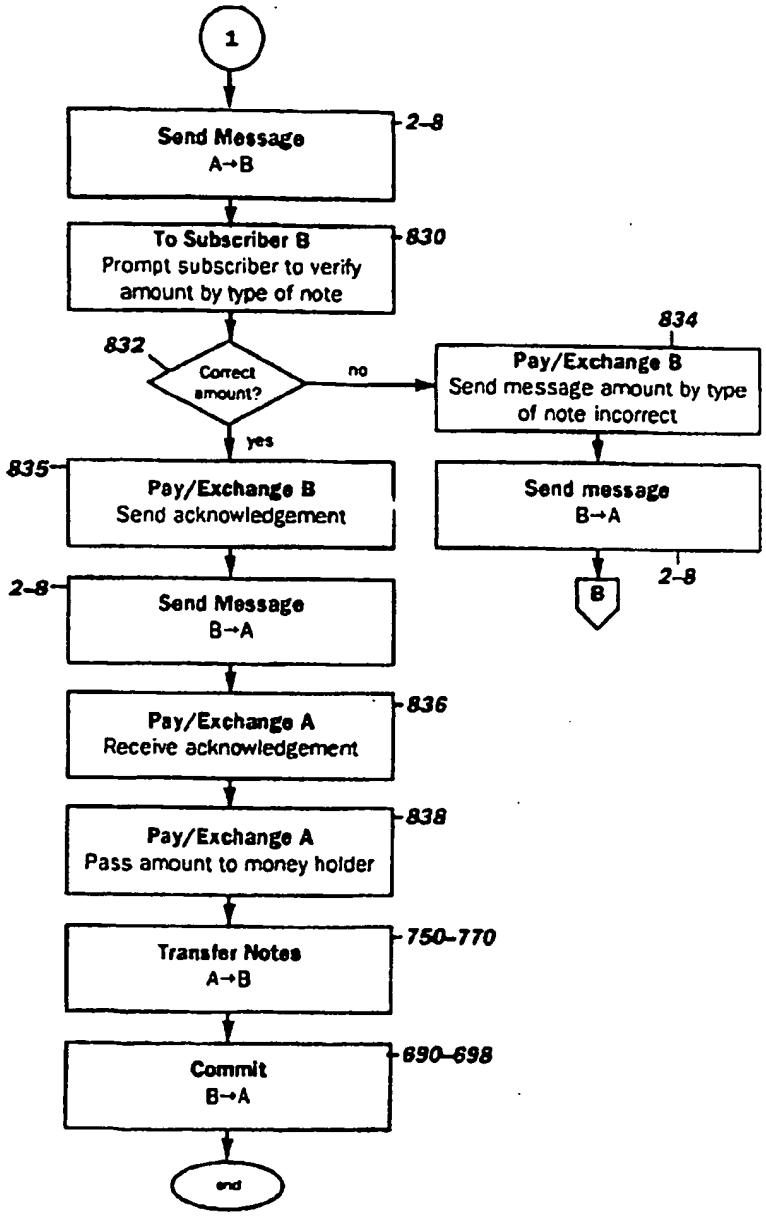
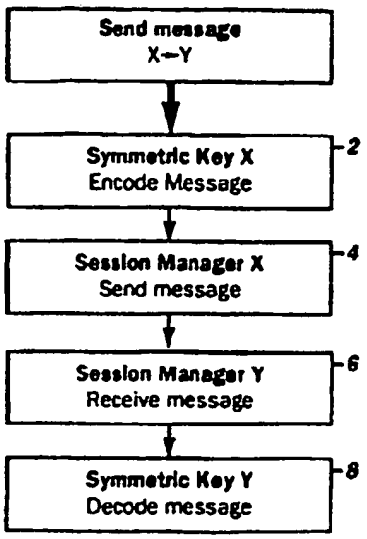

A agrees to pay B an amount
800
A signs on Money Module
10-42
B signs on Money Module
10-42
To Subscriber A
prompt for transaction
806
To Subscriber B
Prompt for transaction
808
A chooses to pay
810
B chooses to receive payment
812
Session manager A
Establish communication
814
Session manager B
Establish communication
816
Establish Session
A←B
190-258
To Subscriber A
Prompt for amount of payment
by type of note
818
A
Pay/Exchange A
Receive amount by type of note
820
B
826
To Subscriber A
Prompt for new amount
by type of note
822
Note Directory A
Check sufficient funds
824
Sufficient
funds?
no
yes
827
New
amount?
yes
A
no
828
Pay/Exchange A
Send message of amount
value to B
Abort Transaction
A←B
500-524
end
1
Subscriber to Subscriber Payment

FIG. 36A



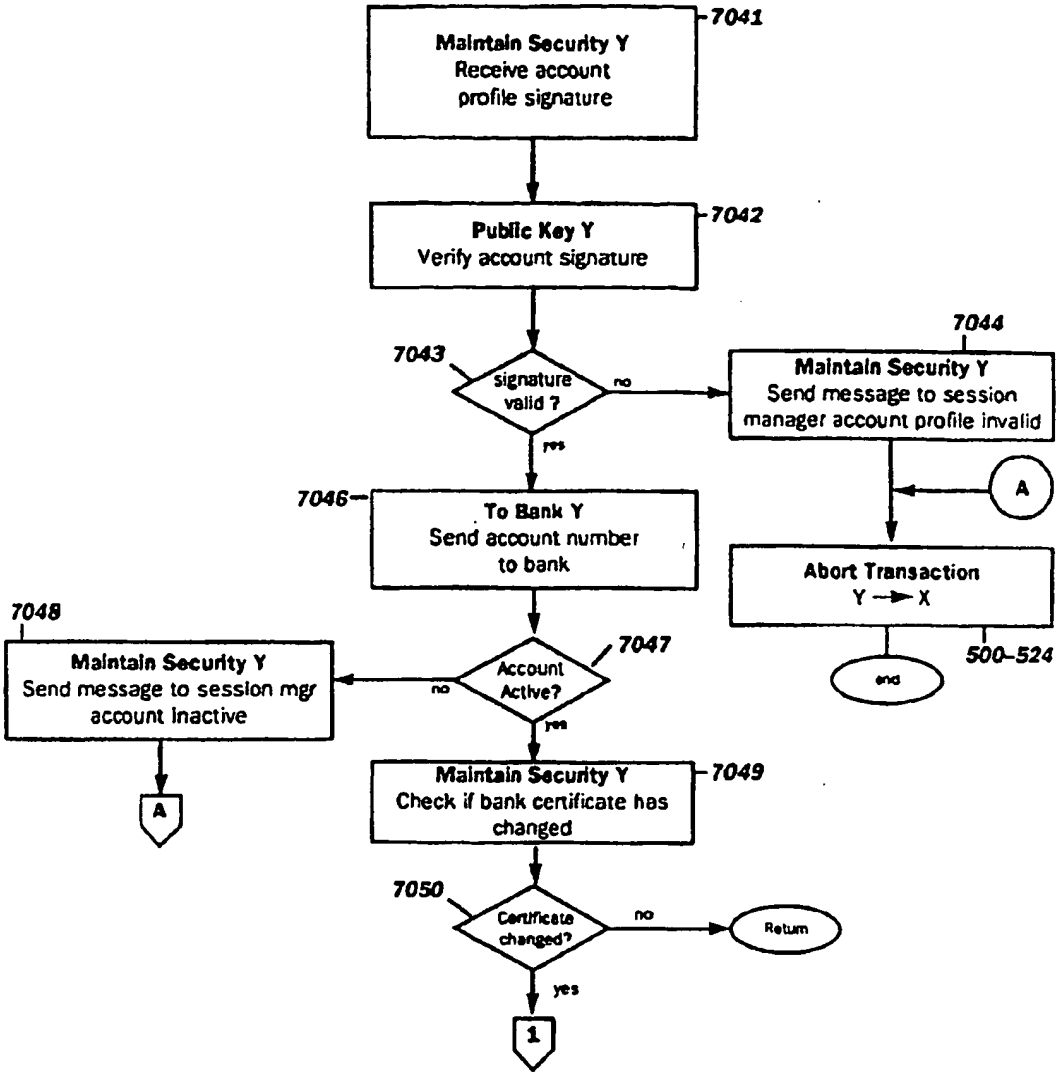
Subscriber to Subscriber Payment (continued)

FIG. 37



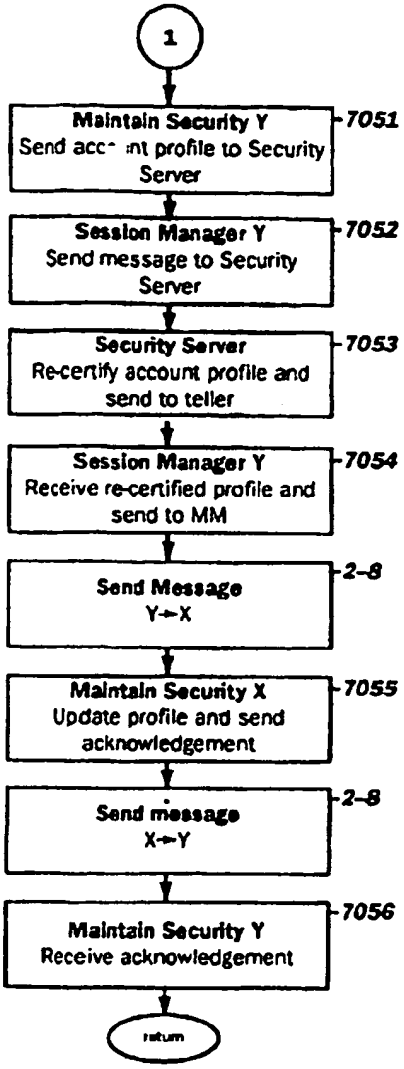
Send Encoded Message — Money Module to Money Module

FIG. 38



Validate Account Number

FIG. 38A



Validate Account Number (continued)

FIG. 39

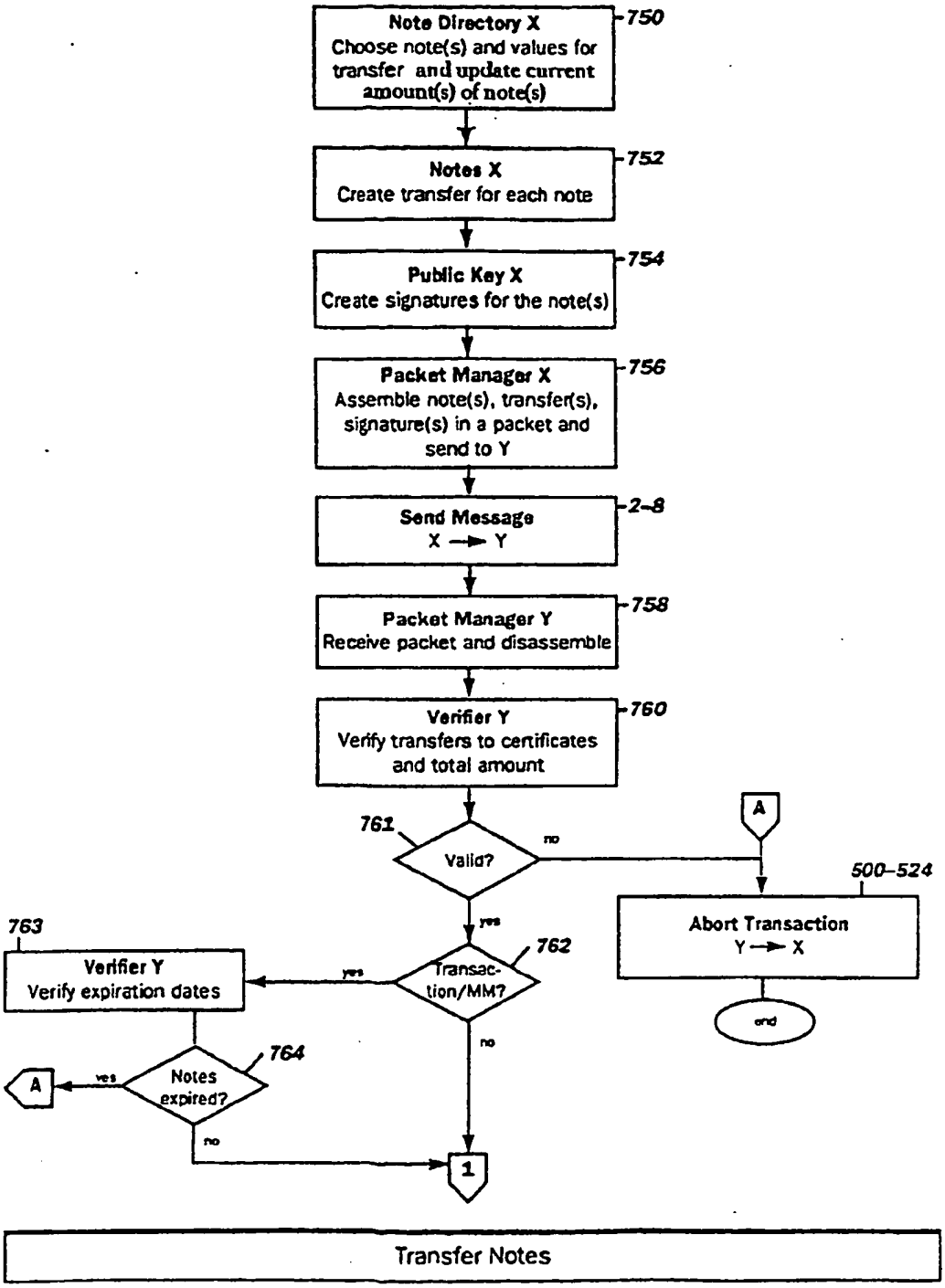
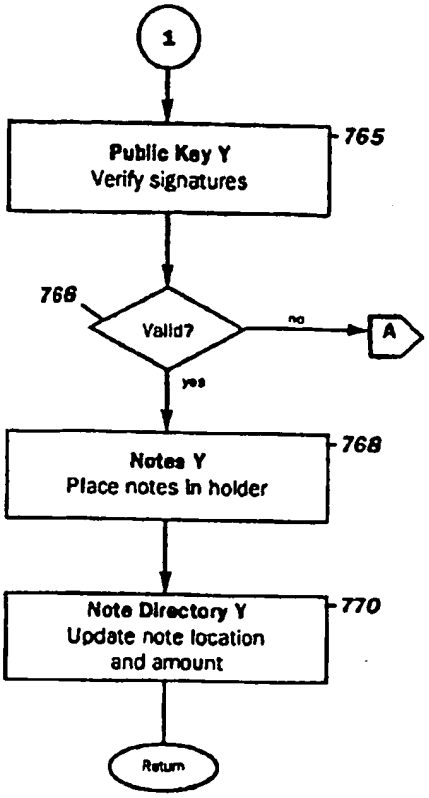
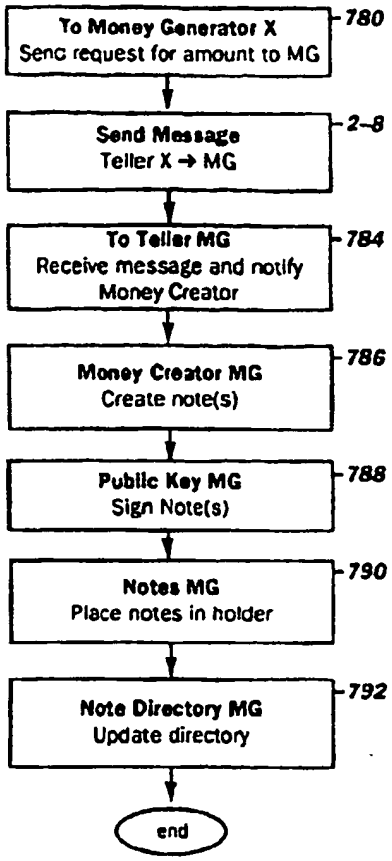

Note Directory X
Choose note(s) and values for transfer and update current amount(s) of note(s)
750
Notes X
Create transfer for each note
752
Public Key X
Create signatures for the note(s)
754
Packet Manager X
Assemble note(s), transfer(s), signature(s) in a packet and send to Y
756
Send Message
X → Y
2-8
Packet Manager Y
Receive packet and disassemble
758
Verifier Y
Verify transfers to certificates and total amount
760
761
Valid?
no
yes
A
500-524
Abort Transaction
Y → X
end
762
Transac-tion/MM?
yes
763
Verifier Y
Verify expiration dates
764
Notes expired?
yes
A
no
1
Transfer Notes

FIG. 39A



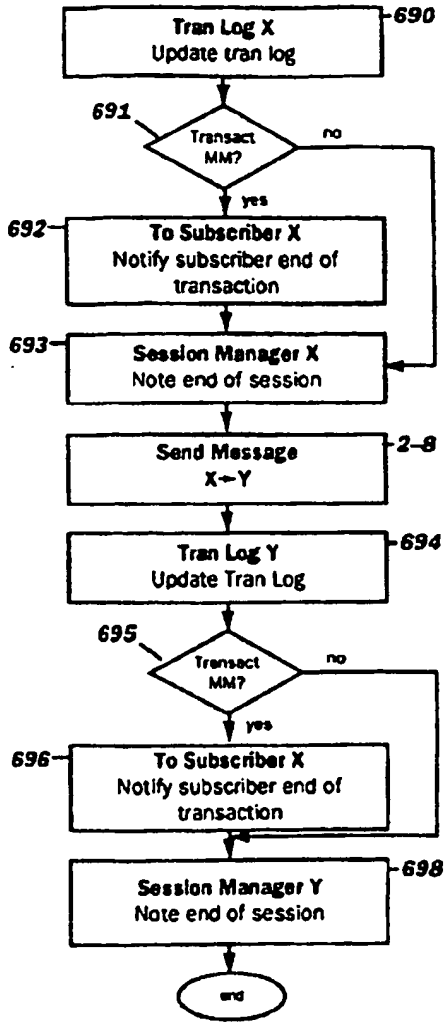
Transfer Notes (continued)

FIG. 4C



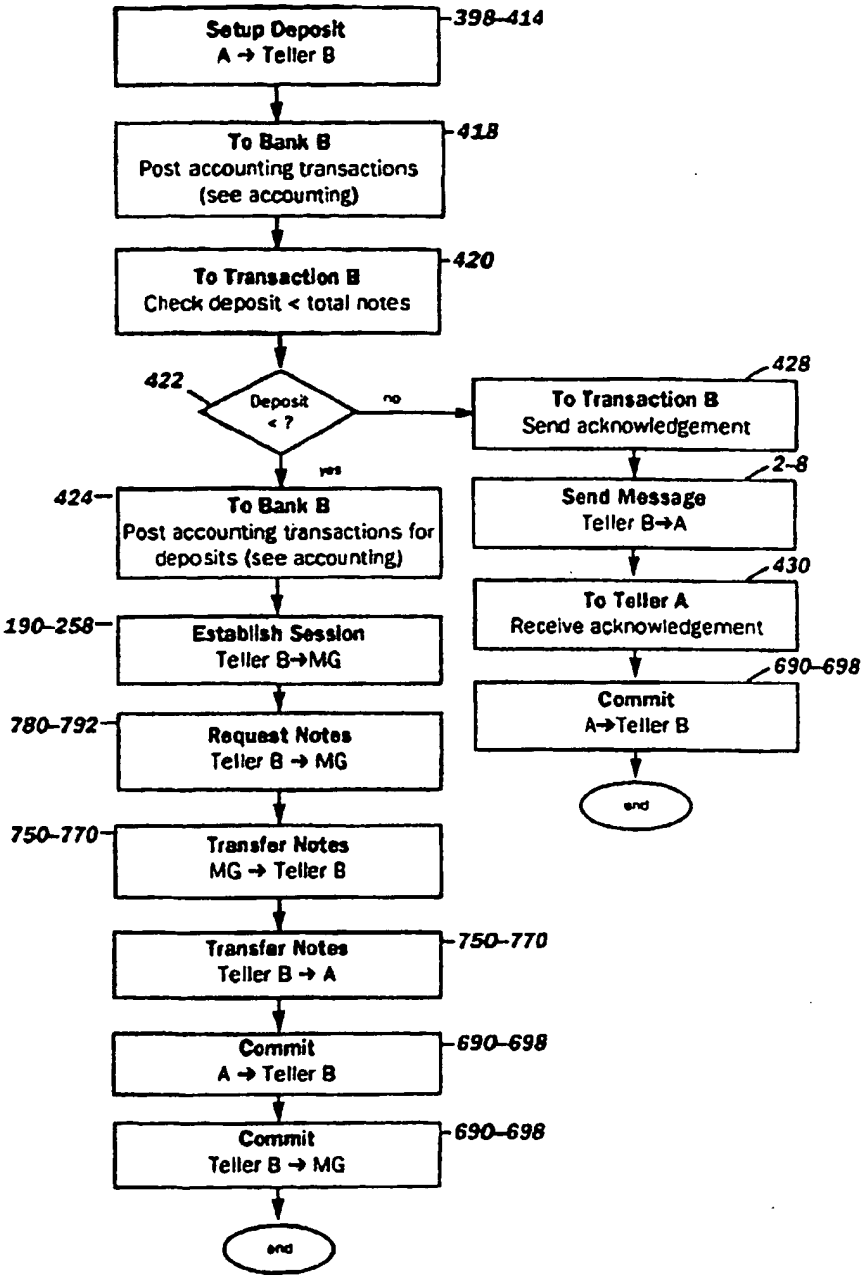
Request Notes

FIG. 41



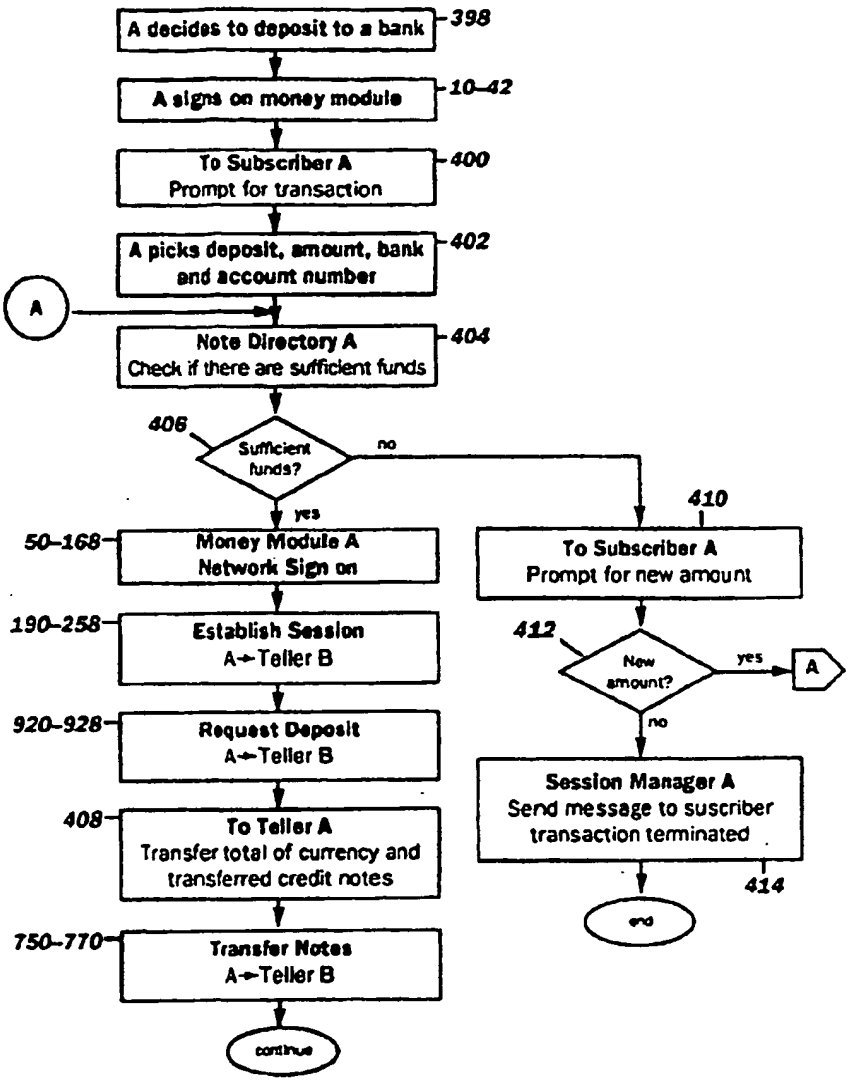
Commit

FIG. 42



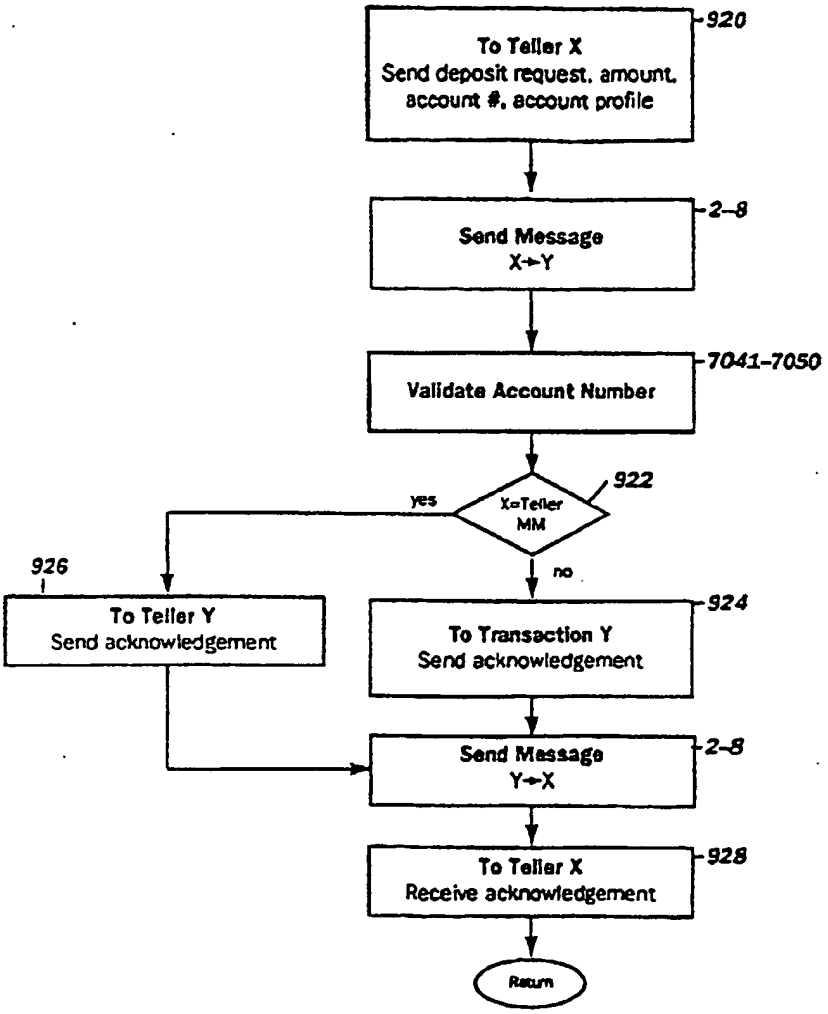
Deposit to Issuing Bank

FIG. 43



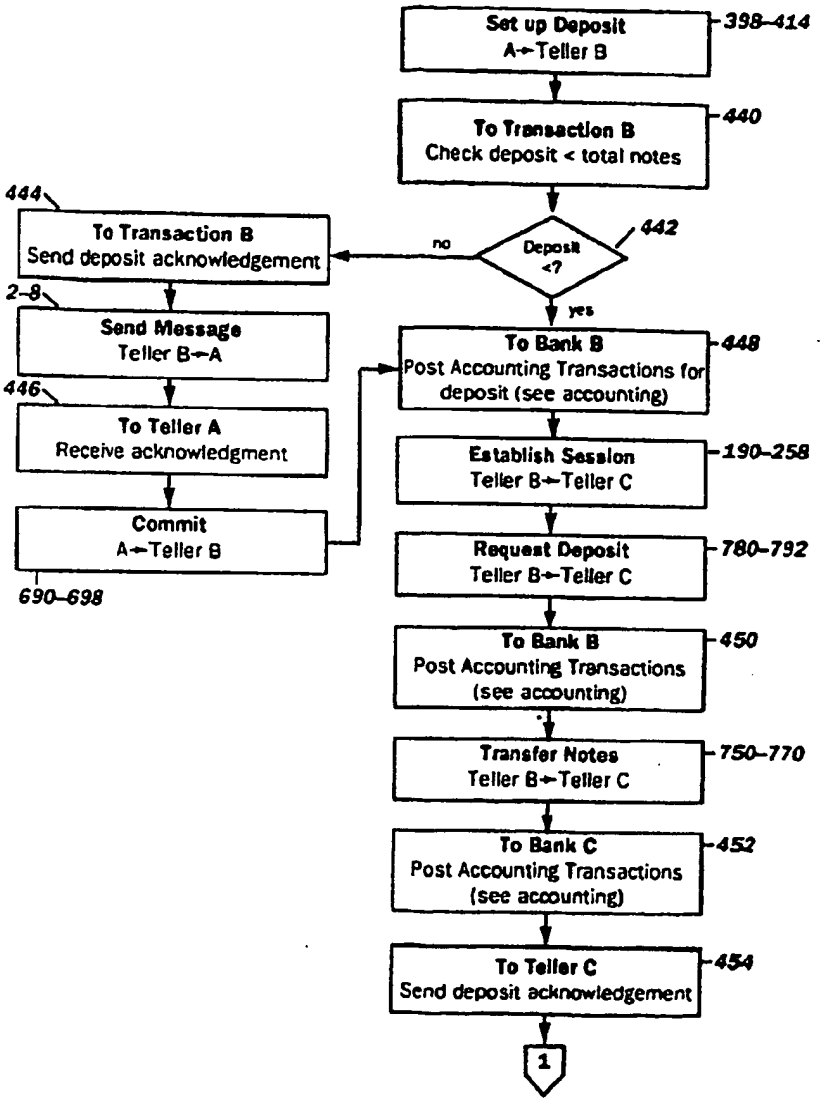
Set Up Deposit

FIG. 44



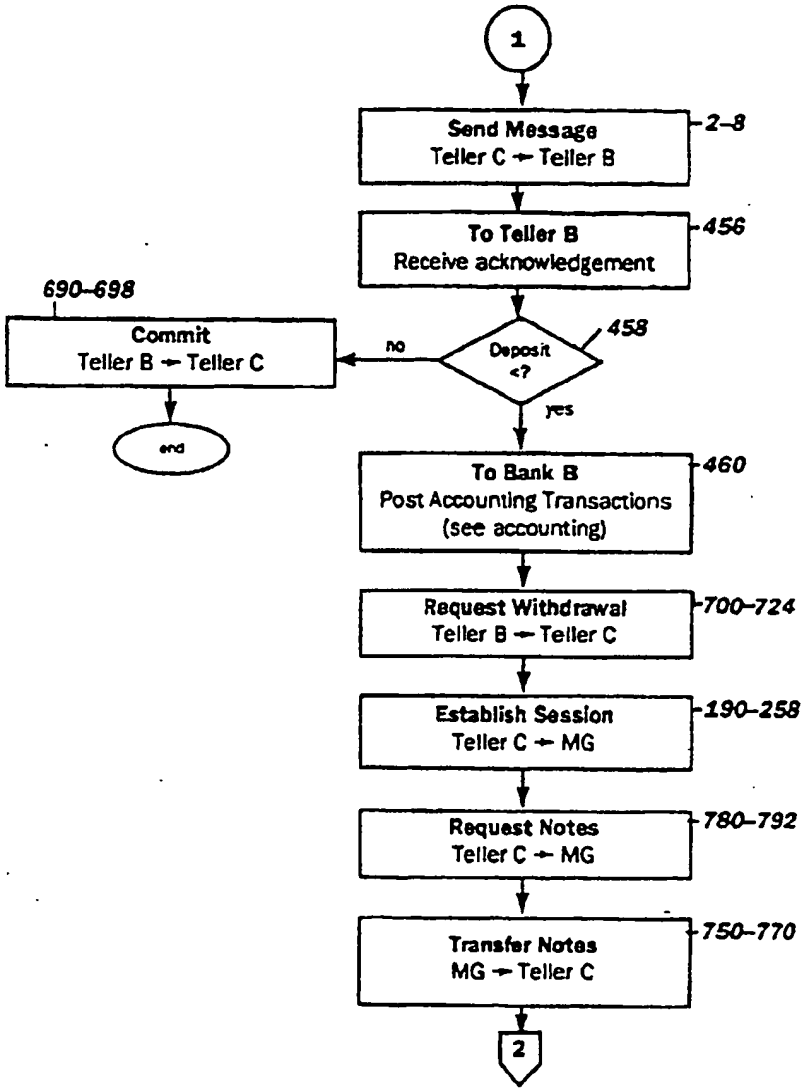
Request Deposit

FIG. 45



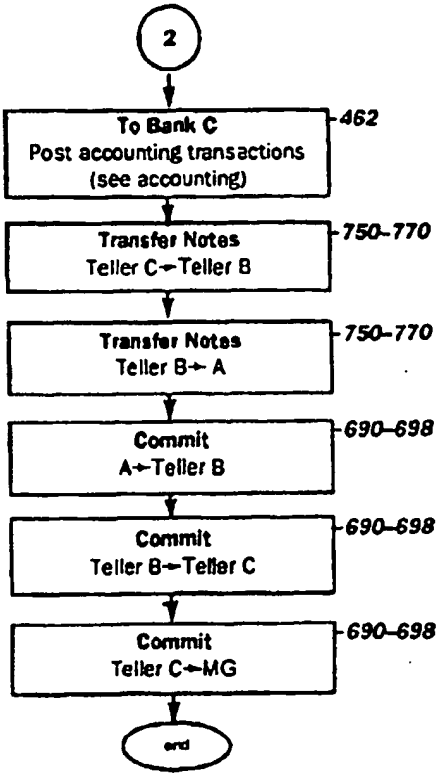
Deposit to Correspondent Bank

FIG. 43A



Deposit to Correspondent Bank (continued)

FIG. 45B



Deposit to Correspondent Bank (continued)

FIG. 46

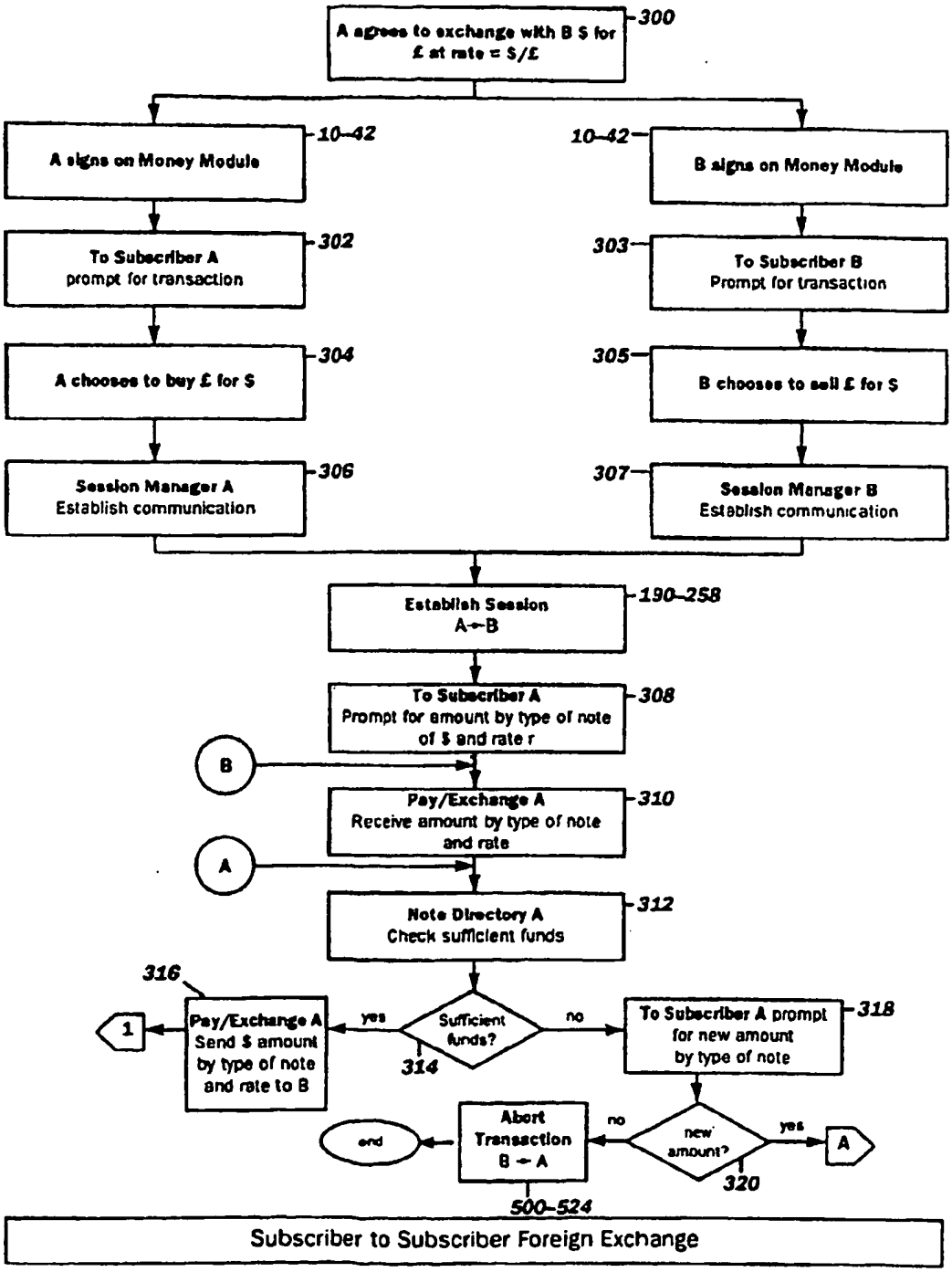
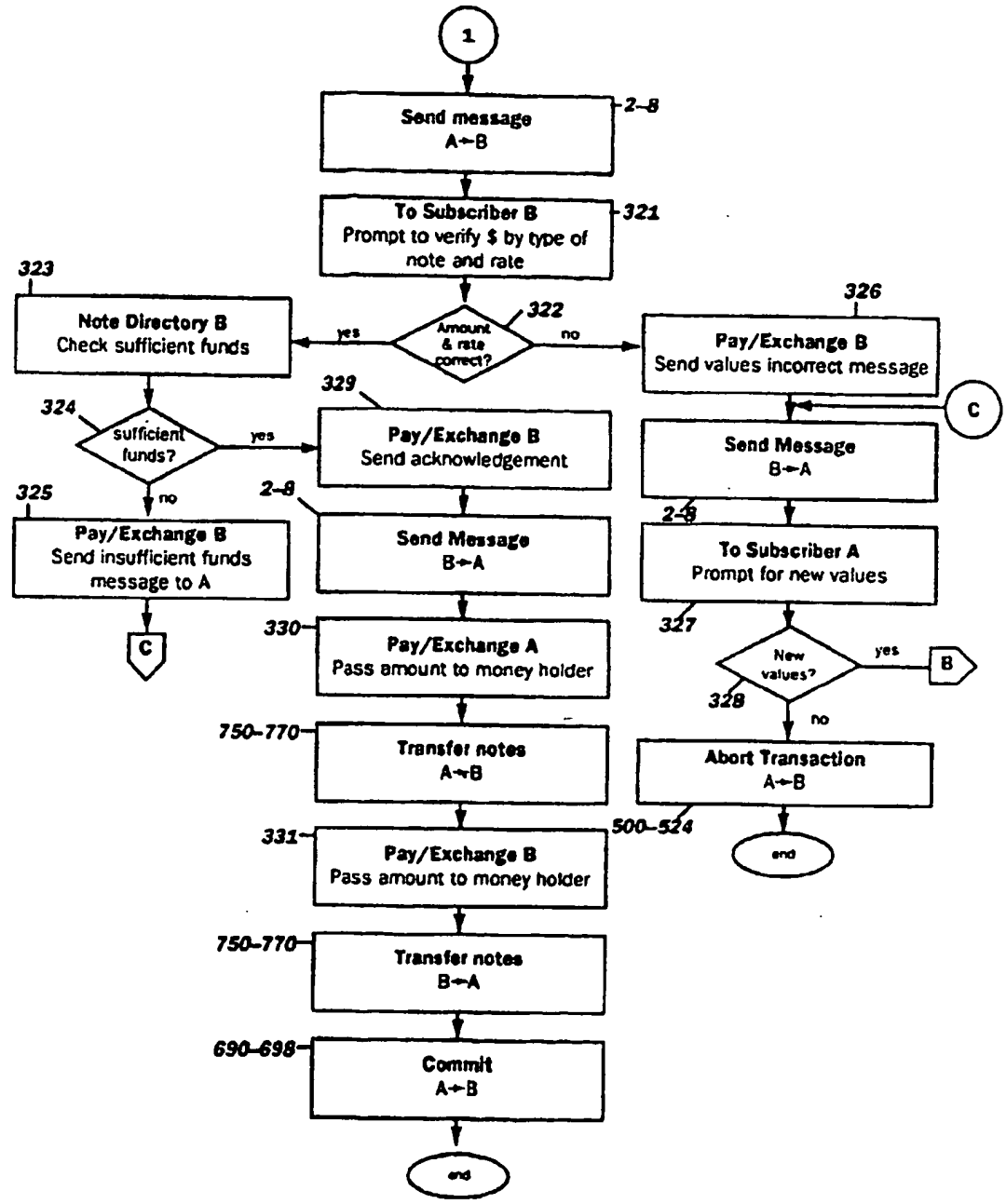

A agrees to exchange with B $ for £ at rate = $/£
300
A signs on Money Module
10-42
B signs on Money Module
10-42
To Subscriber A prompt for transaction
302
To Subscriber B Prompt for transaction
303
A chooses to buy £ for $
304
B chooses to sell £ for $
305
Session Manager A Establish communication
306
Session Manager B Establish communication
307
Establish Session A↔B
190-258
To Subscriber A Prompt for amount by type of note of $ and rate r
308
B
Pay/Exchange A Receive amount by type of note and rate
310
A
Note Directory A Check sufficient funds
312
316
1
Pay/Exchange A Send $ amount by type of note and rate to B
yes
Sufficient funds?
314
no
To Subscriber A prompt for new amount by type of note
318
end
Abort Transaction B → A
no
new amount?
320
yes
A
500-524
Subscriber to Subscriber Foreign Exchange

FIG. 46A



Subscriber to Subscriber Foreign Exchange (continued)

FIG. 47

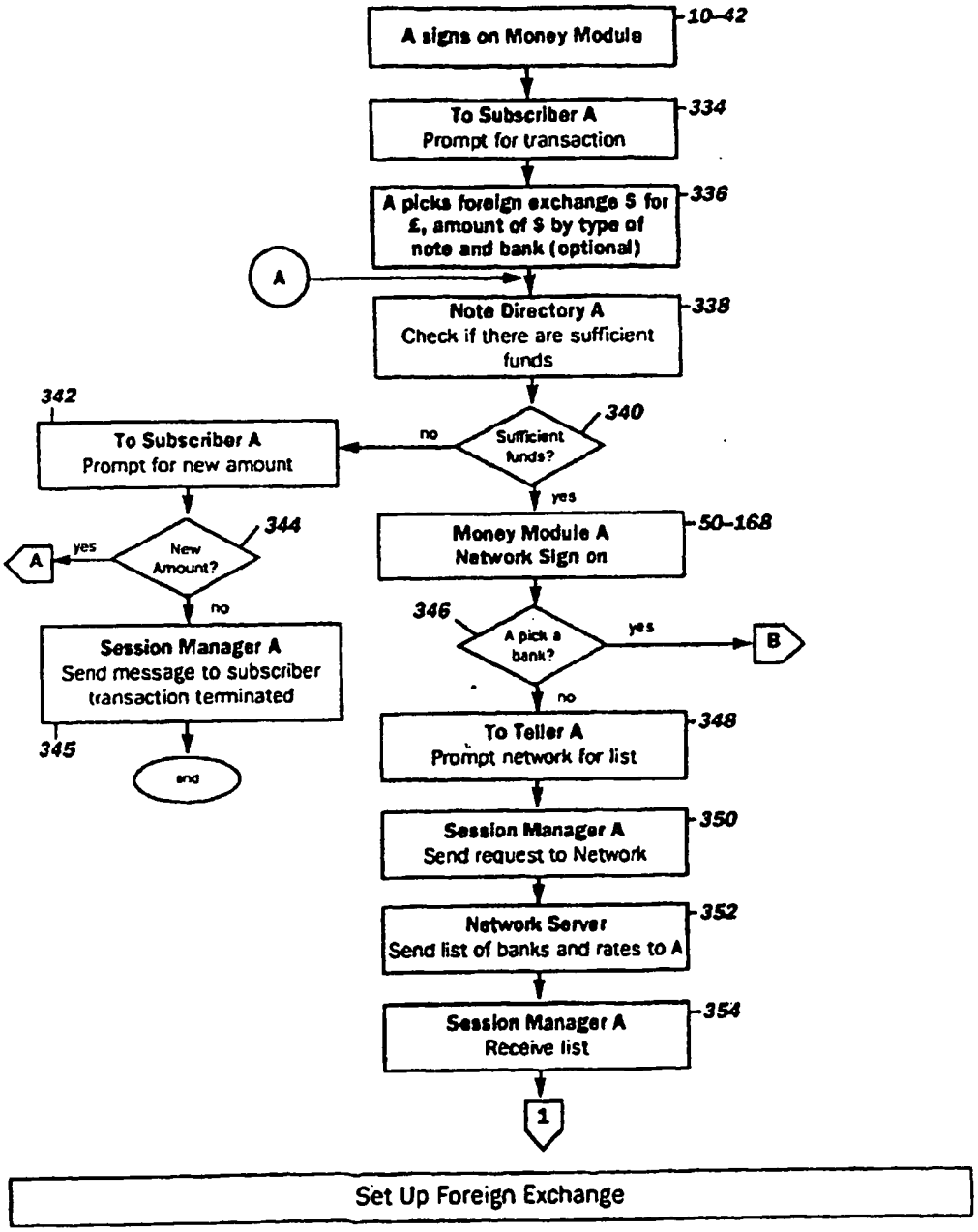
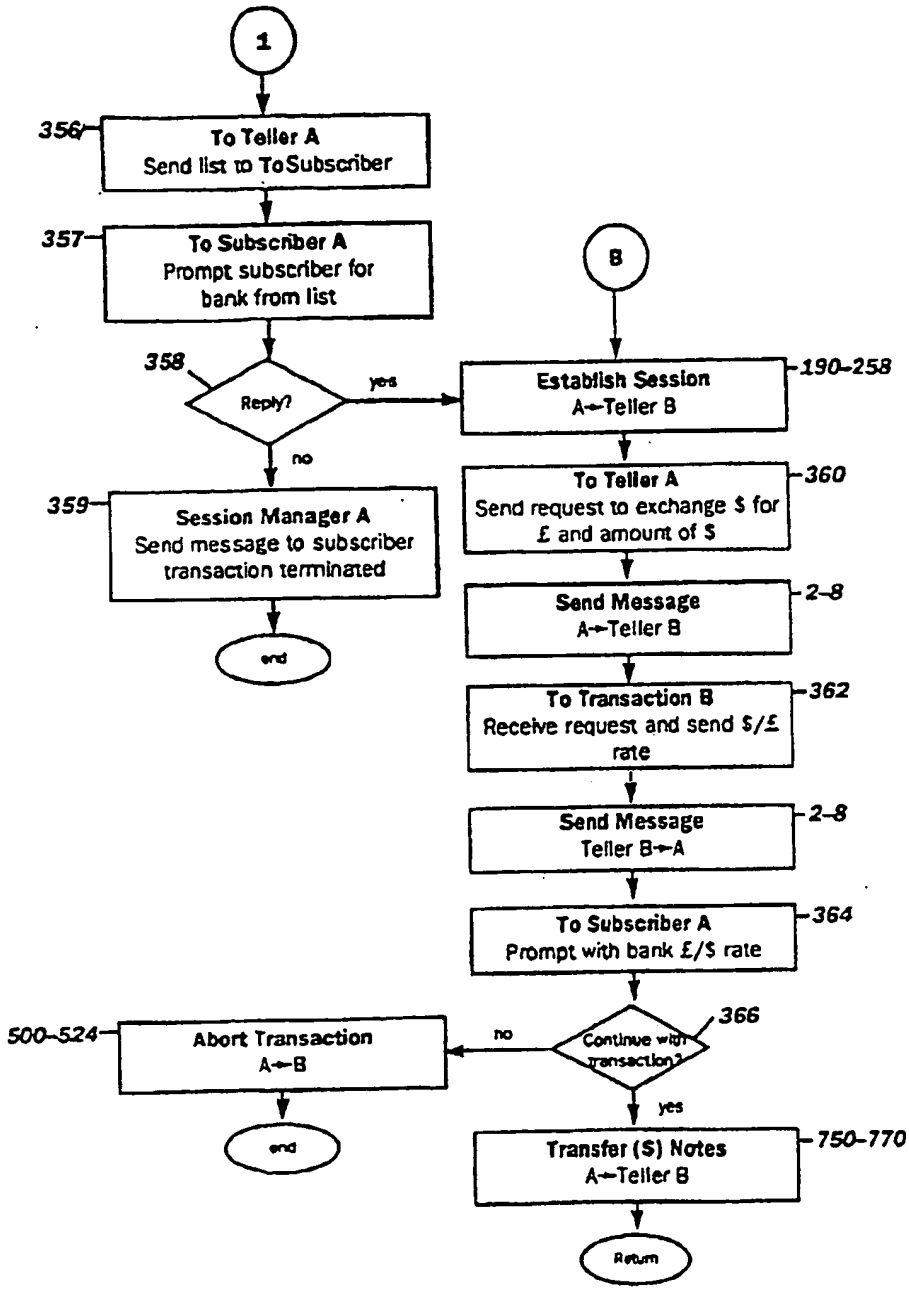
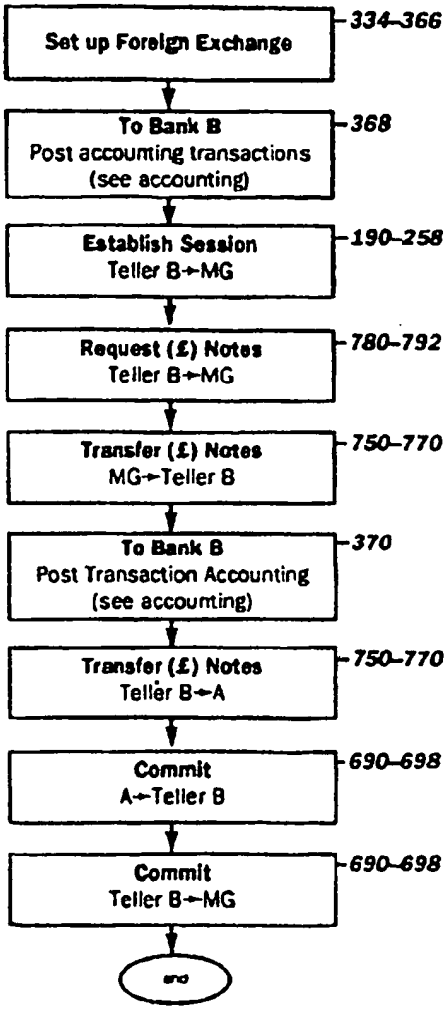

A signs on Money Module
10-42
To Subscriber A
Prompt for transaction
334
A picks foreign exchange $ for £, amount of $ by type of note and bank (optional)
336
A
Note Directory A
Check if there are sufficient funds
338
342
To Subscriber A
Prompt for new amount
no
Sufficient funds?
340
yes
New Amount?
344
yes
A
no
Session Manager A
Send message to subscriber transaction terminated
345
end
Money Module A
Network Sign on
50-168
346
A pick a bank?
yes
B
no
To Teller A
Prompt network for list
348
Session Manager A
Send request to Network
350
Network Server
Send list of banks and rates to A
352
Session Manager A
Receive list
354
1
Set Up Foreign Exchange

FIG. 47A



Set Up Foreign Exchange (continued)

FIG. 48



Foreign Exchange — Issuing Bank

FIG. 4S

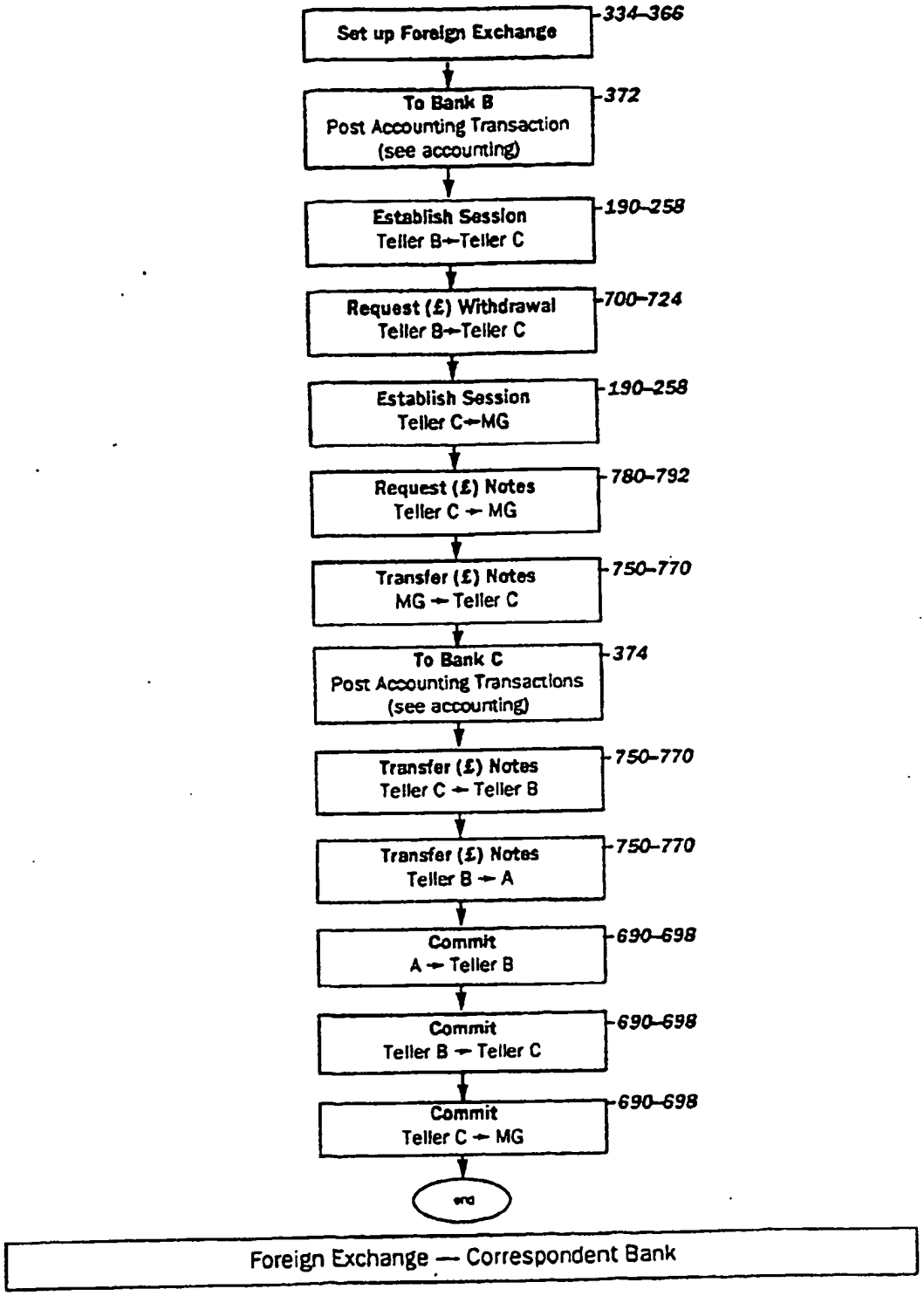
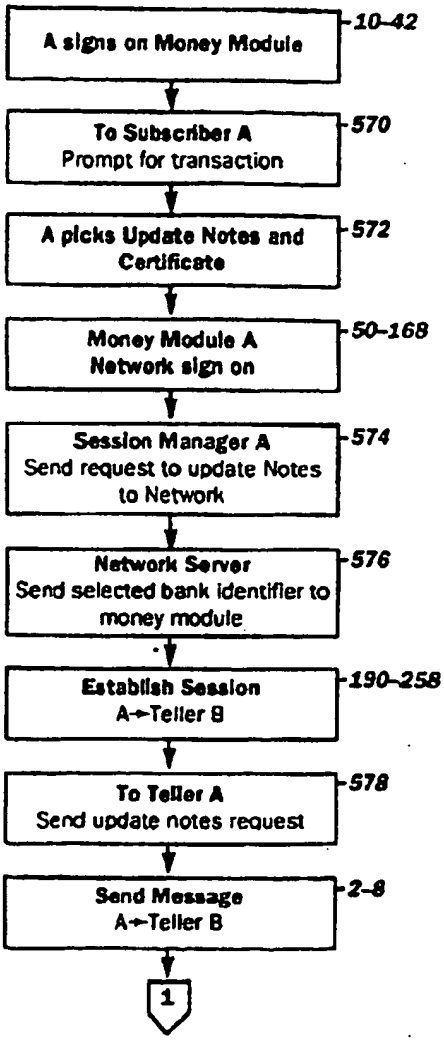
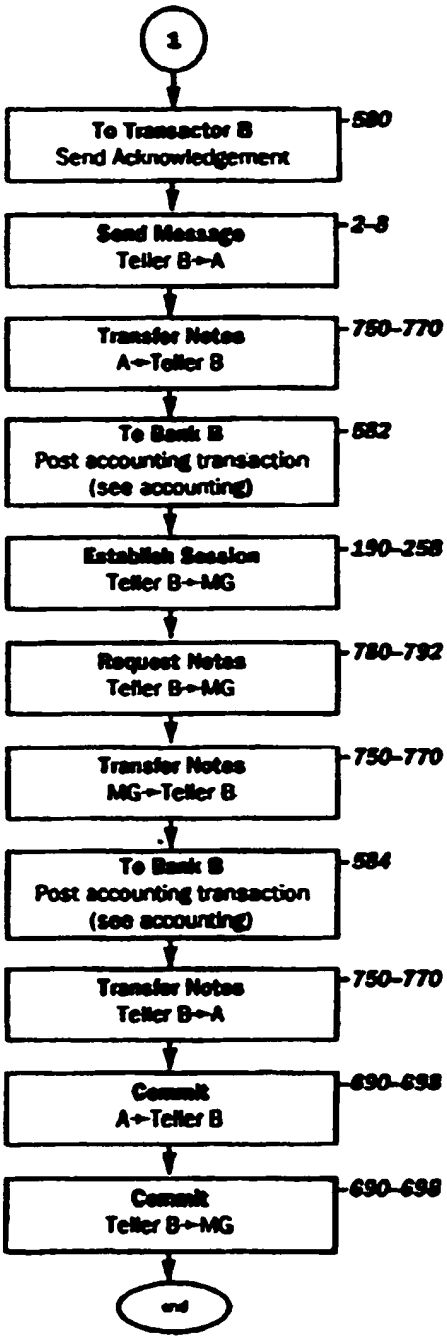

Set up Foreign Exchange
334–366
To Bank B
Post Accounting Transaction
(see accounting)
372
Establish Session
Teller B←Teller C
190–258
Request (£) Withdrawal
Teller B←Teller C
700–724
Establish Session
Teller C←MG
190–258
Request (£) Notes
Teller C ← MG
780–792
Transfer (£) Notes
MG ← Teller C
750–770
To Bank C
Post Accounting Transactions
(see accounting)
374
Transfer (£) Notes
Teller C ← Teller B
750–770
Transfer (£) Notes
Teller B ← A
750–770
Commit
A ← Teller B
690–698
Commit
Teller B ← Teller C
690–698
Commit
Teller C ← MG
690–698
end
Foreign Exchange — Correspondent Bank

FIG. 50



Update Money Module Notes and Certificate

FIG. 50A



Update Money Module Notes and Certificate (continued)